中小型企业

网络管理



——基于Windows平台

刘增杰　张俊斌　编著



全面讲解网络管理配置与部署



共66课全语音讲解
20小时视频教学

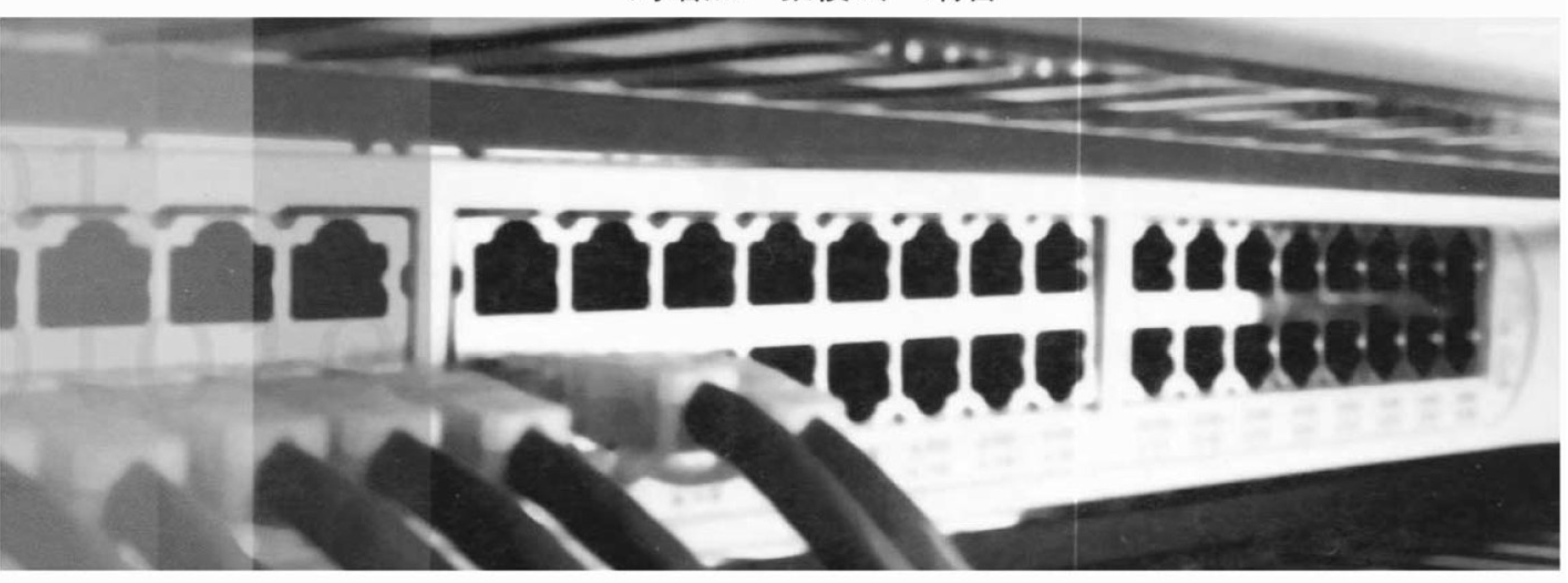
清华大学出版社

中小型企业网络管理



——基于Windows平台

刘增杰　张俊斌　编著



清华大学出版社
北　京

内 容 简 介

本书主要介绍的是针对中小型企业的网络管理和网络安全技术，为了使读者清晰系统地认识网络管理和网络安全，本书将两者分为17章分别讲解。在内容组织上，网络管理首先从网管基础开始介绍，包括网络管理协议的介绍；其次以现实网络管理工程案例为背景进行需求分析及施工方案设计，给出网络管理过程中要实施的管理模块；然后，后面章节的内容根据前面需求分析给出的管理模块分别进行实现。网络安全的内容组织形式和网络管理相似。这种方式可以使读者循序渐进地学习，同时也可以让读者系统地了解现实网络管理及网络安全工程的施工流程等内容，便于读者举一反三，胜任中小型企业的网络管理工作。随书光盘中赠送了20小时培训班形式的视频教学录像，真正体现本书“完全”的含义，令其物超所值。

本书内容丰富全面，图文并茂，深入浅出，使读者能够理解网络管理的精髓，并能解决实际生活或工作中的问题，真正做到知其然更知其所以然。它适用于对中小型企业管理感兴趣的零基础读者，计算机网络技术、网络工程、网络安全相关专业的学生；以及具有一定的网络基础知识，熟悉网络路由交换技术，熟悉网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师。

图书在版编目（CIP）数据

中小型企业网络管理实战宝典：基于Windows平台/刘增杰，张俊斌编著.—北京：清华大学出版社，2011.11

ISBN 978-7-302-26837-6

I. ①中… II. ①刘… ②张… III. ①中小企业－计算机网络－管理 IV. ①TP393.18

中国版本图书馆CIP数据核字（2011）第187061号

责任编辑：夏非彼　马颖君
责任校对：闫秀华
责任印制：
出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：190×260　　**印　张：**34　　**字　数：**871千字
附光盘1张
版　　次：　　**印　次：**
印　　数：
定　　价：

产品编号：

前 言

随着网络技术的发展，中小型企业对于网络的管理与安全越来越重视，因此很多企业希望能招聘到有较高技术水平、实践能力的工程师。面对这种社会需求，很多学校也开设了网络管理及网络安全课程，但是其中的网络管理课程一般都是简单网络扫描软件的介绍，而在网络安全课程方面，大都以安全技术为主要内容，比如加密、认证、安全协议介绍等，对现实中的企业安全管理设备环境的架设涉及比较少。除此之外，在校学生大都停留在技术学习层面，对现实网络工程了解甚少，设备选型、项目施工流程等内容大都处于空白状态。

结合以上问题，如何让有意向成为网络工程师、网络管理员、网络安全工程师的人，在负担较小经济压力的前提下学到有价值的东西，成为了社会的主要需求。

而本书就是针对这一需求定制的。作者在网络工程、网络管理、网络安全方面从事了多年研究及毕业生培训、实训工作，本书由实训经验和企业网络环境总结而来。

本书内容

本书主要介绍的是针对中小型企业的网络管理和网络安全技术，并基于 Windows 的操作系统平台。本书将利用理论联系实际的方法，通过典型的实例向大家介绍网络管理的知识。

第 1 章介绍网络管理的技术基础，包括网络管理的五大职能、体系结构和网络管理实现模式分析等内容。

第 2 章介绍 SNMP 网络管理协议及其配置等。读者想要高效的完成网络管理任务，首先需要掌握 SNMP 协议的运行原理及相关运用技术。

第 3 章介绍中小型企业网络管理项目的需求分析和实施流程。读者想要实现完善的网络管理体系，必须掌握网络管理方案的设计原理。

第 4 章介绍网络基本信息的获取方法，并通过两个项目实例进行详细讲解。

第 5 章介绍主流网络管理平台的架设和应用，使读者掌握高效管理网络的方法。

第 6 章介绍服务器远程监控与管理，使读者掌握高效管理远程服务器的方法。

第 7 章介绍网络流量监测分析的工具及其使用方法，使读者掌握利用流量监测分析工具发现网络异常的方法。

第 8 章介绍企业网络主流监控产品及其使用方法，使读者掌握利用网络监控产品进行网络监管的方法。

第 9 章介绍网络安全的基础知识，包括攻击类型及防护策略。

第 10 章介绍企业网络安全项目分析和实施流程，使读者掌握中小型企业网络安全方案的设计原理。

第 11 章介绍 Windows Server 2008 系统安全及策略，使读者掌握系统安全的配置方法。

第 12 章介绍网络设备安全概述及其配置。

第 13 章介绍无线网络安全现状及其实施措施，使读者掌握小型无线局域网的使用及安全配置。

第 14 章介绍企业防火墙架设及配置，使读者掌握中小型企业防火墙的架设与应用方法。

第 15 章介绍反病毒系统及其配置实例，使读者掌握解决企业病毒威胁的方法。

第 16 章介绍 VPN 技术的概述及分类，使读者掌握使用 VPN 技术保证信息在互联网安全传输

的方法。

第 17 章介绍入侵检测系统的概述及分类，使读者掌握网络入侵安全问题的解决方法。

本书特色

理论联系实际：网络管理及网络安全均添加中小型企业中用得到的案例，以基础知识开始引入，帮助读者了解该项网络技术。本书采用中小型企业中使用较多，安全性、稳定性较高的软硬件产品工具。

一步一图，图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

易学易用：颠覆传统“看”书的观念，变成一本能“操作”的图书。

举一反三：同一类技术或产品，大都会介绍至少两款主流工具产品供读者学习使用，从而更加深刻理解网络管理知识，达到触类旁通的效果。以中小型企业环境为基础，同时兼顾必备的基础知识及设计原理，进而达到“知其然，并知其所以然”的效果。

实训效果：本书采用案例介绍、需求分析、实施流程规划及分步施工的顺序组织内容，方便读者系统的、模块化的学习，使读者通过阅读此书，能够达到网络实习的效果。

超值光盘：随书奉送 20 小时的培训班形式的视频教学录像，使本书真正实现“自学无忧”，成为一本物超所值的好书。

读者对象

本书是一本完整介绍中小型企业网络管理应用知识的教程，内容丰富，条理清晰，实用性强，适合以下读者学习使用：

- 对中小型企业管理感兴趣的零基础读者；
- 计算机网络技术、网络工程、网络安全相关专业的学生；
- 具有一定的网络基础知识，熟悉网络路由交换技术，熟悉网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师；
- 各行各业需要学习网络管理知识的人员。

鸣谢

本书作者长期从事网络实训的培训工作。参与本书编写人员除了封面署名人员以外，还有王英英、苏士辉、肖品、张少军、孙若淞、宋冰冰、王维维、梁云亮、程铖、臧顺娟、刘海松、陈伟光等人。虽然倾注了编者的努力，但由于水平有限、时间仓促，书中难免有错漏之处，请读者谅解，如果遇到问题或有意见和建议，敬请与我们联系，我们将全力提供帮助，编者电子邮箱为 liuyu_200882@163.com。

编者

2011 年 7 月

目　录































15.1 反病毒系统概述.avi/10 分钟

15.2 项目实施 1.ESET NOD32 企业反病毒系统实战案例.avi/49 分钟

15.3 项目实施 2.趋势科技企业反病毒系统实战案例.avi/70 分钟



16.1 VPN 技术介绍.avi/13 分钟

16.2 基于 Windows 的远程访问 VPN.avi/32 分钟

16.3 基于 ISA 防火墙的 VPN.avi/41 分钟



17.1 入侵检测系统的概述.avi/18 分钟

17.2 入侵检测系统系统分类.avi/17 分钟

17.3 项目实施 1.入侵检测系统工具实战.avi/9 分钟

17.4 项目实施 2.提高网站服务器的安全.avi/12 分钟

第 1 章　网络管理技术基础

从上世纪 90 年代开始，国内网络事业蓬勃发展，网络技术也逐步普及。到目前为止，网络几乎无处不见，在生活、工作中越来越多的人离不开网络。由于网络环境不断的普及壮大，相应的网络管理问题也越来越被重视。在这种环境下，网络管理技术得到不断的更新、改善。

究竟什么是网络管理技术，应当如何进行网络管理呢？下面对这两个问题进行详细介绍。

1.1　网络管理概述

网络管理，是指网络管理员通过网络管理程序对网络的运行状态进行检测和控制，从而使网络有效、可靠、安全、经济运行的技术体系。从定义来看，网络管理主要包括两部分任务：检测网络运行状态和控制网络运行状态。通过这两部分任务可以了解网络运行是否正常、是否存在潜在危险和瓶颈，并通过控制调节做到优化网络、提高性能、保障服务。可以看出控制和检测是密不可分的，检测是基础，控制做补充。

随着企业信息化不断的发展，依赖于计算机网络和计算机终端的业务及应用越来越多。为了提高业务及应用质量，对于网络设备、终端客户机、服务器、应用程序的性能和可靠性要求越来越高，相应的网络维护管理工作也越来越复杂。

由于信息化发展迅猛，很多企业在应对需求、扩充网络环境及应用复杂性的同时，并不能及时的补充相应的管理人员。在这种相对不和谐的工作环境下，如果可以介入专业的管理技术，高素质的管理人才，会极大的提高网络环境的可靠性、网络应用的高效性。

企业业务对网络的依赖越来越大，一旦出现问题，会造成很多方面的损失。因此，对网络的稳定性、安全性、可靠性、可用性等特征的等级要求也越来越高。企业的业务运作是一整套的东西，如果某一个环节出现网络故障，很可能导致工作停滞。

想要保持网络的稳定性，需要在网络故障发生之前及时发现故障隐患，并能在故障发生之后及时地找出故障原因和解决办法。同时网络的稳定运行也和其性能息息相关，所以需要实时的监控其性能状态，及时地发现性能瓶颈、找到解决办法。

在网络管理过程中，由于网络设备繁杂，单靠人工管理很难应付，所以需要管理员能够智能化的对所有设备进行配置查看和修改。

网络管理是对网络上资源的集中管理，通过对管理内容的细化，可以分为以下五种管理职能：配置管理、性能管理、故障管理、计费管理、安全管理。

1.2 网络管理的发展

伴随网络环境的不断扩大，网络应用的增加，网络结构变得越来越复杂。在这个变化中，网络管理的工作内容也变得越来越有难度，越来越繁重。早期的完全依靠手工实现的网络管理时代早已不能满足网络可用性、稳定性、安全性的需求。紧接着，利用软件实现的简单集中式网络管理模式诞生了，但是网络不断扩大，复杂的网络环境逐步走向分层式网络结构，集中式的网络管理软件已经无法处理剧增的庞大网络管理信息，网络管理再次变得被动。面对广大企业网络管理的需求，分布式、分层的网络管理模型诞生。在这样的发展过程中，网络管理技术不断的被完善。网络管理技术发展至今，已经成为了一套完整的技术体系，并且还在不断的壮大中。

随着网络的壮大，网络应用技术的增加，网络复杂性的提高，网络管理水平和深度的需求，网络管理内容也在不断地增加，各种有针对性的网络管理系统软硬件设备纷纷涌现。根据网络管理内容的不同，网络管理技术可以划分为六个发展方向。

1. 网管系统（NMS）

这个方向产生的产品也可以称作网络运维系统或网络管理平台，主要致力于网络设备的实时监测、配置管理和故障诊断。可以实现网络拓扑自动发现、设备远程配置、各种性能图标的显示、故障报警和分析。目前市场上比较流行的网管系统产品有 HP OpenView、IBM Tivoli NetView、CiscoWorks2000 等。

2. 应用性能管理（APM）

主要用于实现企业关键性业务的性能监测和优化。从原来只监控服务器硬件及系统程序性能，发展到兼顾客户端相应速度，可以实现应用系统各个组件的性能监控，最终可以达到提高企业应用服务可靠性和客户服务质量的目的。目前市场上比较流行的应用性能管理产品有 BMC、Quest 系列产品、Topaz 和 SiteView 等产品。

3. 桌面管理系统（DMI）

主要用于实现对最终用户的全方位管理，包括计算机组件、操作系统、地址信息。可以实现对设备资产信息、软件分发和远程控制等方面的工作，减少了管理员的工作量，提高了工作效率。目前市场上比较流行的桌面管理系统有 CA Unicenter、NetInhandLANDesk Management Suite 7、Landesk 等。

4. 员工行为管理（EAM）

主要用于对员工上网及桌面操作行为的监控和管理。可实现规范员工工作习惯，提高员工管理水平。目前市场上比较流行的员工行为管理系统有 WebSense、NetManage 等。

5. 安全管理

主要用于实现保障合法用户对网络资源的安全访问，防止网络被恶意攻击和破坏。主要通过各种软硬件产品的身份验证、加密认证、访问控制、流量分析、漏洞扫描和安全日志等功能来实现

网络安全保护。

目前市场上比较流行的安全管理系统有：防火墙（Cisco ASA、天融信、NetScreem、Check Point）、IDS 入侵检测（RealSecure、ITA、ESM）、防毒墙（启明星辰、趋势科技）、流量监测分析（Sniffer Pro、科来）、VPN（安达通）、CA 认证等。

1.3 网络管理的五大职能

在进行网络管理时，需要管理的内容、信息繁多，综合起来可以实现五个方面的管理职能，分别是配置管理、性能管理、故障管理、计费管理、安全管理。这五大管理职能的具体内容介绍如下。

1.3.1 配置管理

配置管理在网络管理中非常重要，通过这项功能可以对网络里所有设备进行配置查看、调试、保存等操作，这样一方面提高了设备配置效率，另一方面确保了设备配置的准确性和安全性。配置管理系统需要具备以下功能。

1. 配置管理设备的配置信息

网络环境越来越大，需要配置管理的设备也越来越多，如果所有设备的配置信息全部由人工来完成，工作量会很大，同时由人工操作难免会出现配置错误。而且在设备配置结束后，即便是当初的配置人随着网络环境的逐渐扩充、变换，也不一定能一直掌握所有设备的配置情况，如果换了新的网络管理员，就更不可能掌握整个网络配置了。所以，在实施网络管理时需要架设一套可以实现设备远程配置并可以自动获得管理所有设备配置信息的程序。

当然并非所有配置内容都可以实现远程配置，比如网络设备初始安装时，远程管理端根本无法连接，最基本的连接配置还需要管理员手工操作完成。

2. 自动更新、保存配置

网络管理过程中经常会出现一些需要定期调整的配置内容，比如程序升级。还有设备的配置也会经常地被调整，一旦设备出现故障，原有的配置信息可能会丢失，必须对这些配置信息执行定期备份保存操作。这些周期性的工作内容，如果每次都需要管理员去操作很浪费时间，也很容易忘记。所以，需要专门的管理程序能够定期的自动执行任务计划，以完成这些工作。

3. 配置一致性校验

网络环境较大的情况下，需要配置的设备太多，一般都会由多人完成配置，虽然前期有详细的配置方案，但是在实施过程中难免会出现问题。再者，在日常网络维护中，网络环境或设备会经常被改动，在改动过程中也难免出现错误的配置。这些情况都有可能导致网络无法正常使用。所以，在网络管理过程中要经常对网络设备的配置进行一致性校验。其中对网络使用影响较大的配置内容主要是路由器、交换机、防火墙等关键设备的配置。

4. 配置变化记录

网络中有一部分设备需要被用户频繁使用，而这部分设备很容易被普通用户操作错误的配置信息，一旦设备出现故障在，在没有任何资料的情况下，网络管理员进行故障排查会很吃力。如果可以实时的记录设备配置信息的变化情况，管理员就可以通过这些记录信息迅速的查出导致故障的错误配置。这一般可以通过设备的系统日志功能来实现，管理员通过远程管理可以查看保存这些日志信息。

1.3.2 性能管理

性能是用来评价系统、设备和网络整体运行状况的重要信息。这些性能信息如果能被合理利用，网络管理员就可以及时地发现性能瓶颈、故障隐患及原因。而网络管理系统就可以提供性能管理机制，帮助管理员进行性能检测分析，并对异常现象报警。详细剖析，性能管理系统需要具备以下功能。

1. 性能监控

设备、系统和网络的性能需要由专业的工具统计产生，最终可能产生的性能信息有 CPU 使用率、空闲内存量、磁盘驱动器读写速率、网络流量、丢包率、网络延迟等，这些性能信息通过性能管理程序的处理可以生成性能报告。

2. 性能分析

获取性能信息和性能报告的意义在于查找性能瓶颈和故障隐患。这需要对已统计的性能信息进行整理、分析，并和性能指标做比较，最终得出分析结果和调整方案，使整个网络的性能得到最好的发挥。

3. 警报阈值控制

设备、系统和网络出现异常时，性能状态会有所改变，如果当时没有进行性能监控和分析，很可能使异常恶化。通过性能管理程序，可以设定性能阈值，一旦监控到的性能信息超过了设定的阈值，代表出现了异常，并向管理员发送警报提示。

1.3.3 故障管理

网络故障一直是网络管理员最头痛的问题，有些故障可能会造成巨大的损失，而有些故障不大，但却频繁发生。不过一般的网络故障都是一些小故障，这些小故障虽然危害不大，但是恢复起来也需要管理员费一番手脚，关键是这些小故障发生的频率都很高，时间长了就变成了占用管理员时间最多的、机械的、重复的工作。

其实网络里的每一个用户和管理员的期望都一样，希望故障彻底消失。但是这不可能，作为管理员能做的是尽量避免故障发生，尽快解决故障。当没有故障时，管理员需要实时的监控网络，分析故障隐患，让故障结束在萌芽状态。当故障发生后，管理员需要第一时间让网络畅通，然后再查找故障原因进行恢复。

要做到以上内容需要架设一套完善的故障管理系统，通过该系统实现故障检测、隔离和恢复。

详细剖析，故障管理系统需要具备以下功能。

1. 故障监测

首先故障管理系统要能够发现故障，通过设备系统自身的事件和审核功能可以发现故障并将其以事件日志的形式记录。通过网络性能和流量分析程序也可以获得网络故障信息。

2. 故障报警

发现网络故障之后，如果不能及时被管理员获知，故障就会继续威胁网络，需要使用故障管理系统向管理员发送报警信息。报警信息可以通过提示窗口、提示音、电子邮件等多种方式告知管理员。

故障报警需要根据故障的大小，按照不同的级别进行处理，这样有助于管理员合理安排恢复优先级。

3. 检索 / 分析故障信息

管理员获知故障事件后，需要对各种日志和其他记录信息进行故障分析，找出故障原因。

4. 排错支持工具

在分析故障原因时，可能出现的原因比较多，需要使用不同的方法或工具进行故障测试，找出真正的原因。这需要使用各种针对性的排错工具。所以架设故障管理系统时必须准备这方面的工具程序。

1.3.4 计费管理

网络资源是有限的，如果无限制地被使用，根本不可能满足需求，所以在网络资源限制较明显的位置应该架设计费管理系统。通过计费管理系统可以评估出用户使用网络资源需要支付的费用和代价，限制用户能够使用的网络资源等。比较常见的计费管理系统应用有网吧上网时间费用记录、银行系统网络流量计费等。详细剖析，计费管理系统需要具备以下功能。

1. 采集计费数据

计费的依据主要是网络中的流量数据，所以计费管理系统必须要支持一定的计费信息搜集功能。该项功能的支持可能会受到硬件设备和软件的限制无法实现，管理员需要留意。

2. 数据分析与费用计算

获得计费信息后，需要对数据进行分析获知用户的网络资源使用情况，进而判断其应该交纳的费用。

3. 计费数据的管理和维护

扫描到计费信息后，经过统计要实现费用的交纳、资源使用的规则配置等工作，这需要人为的管理。比如用户交费能够支持多久、多大带宽、多少流量的资源使用，如何确保用户不超额使用。

4. 计费业务交易平台

用户作为消费者，有权选择自己使用的计费业务，需要计费管理系统提供这种业务功能。同时，用户在支付费用时，有权获知自身的网络资源使用情况，并能通过这些信息核算自己需要支付的费用。

1.3.5 安全管理

网络安全虽然一直被强调，但是它依然是大部分网络的薄弱环节。由于网络安全威胁越来越大，想要保障安全，必须配置一套完整的安全管理系统，该系统可以包括认证口令、安全设备、访问控制规则、安全协议、日志记录与分析、漏洞监测分析、警报策略等内容。下面依次介绍这些功能。

1. 认证口令

无论是网络设备、操作系统，还是应用程序，都有设置身份认证、登录口令等配置内容，这些内容属于最基本的安全防护内容。但是这些配置很重要，管理员需要一套安全的身份认证加密技术和口令复杂性配置方法，并且，配置的认证口令需要进行系统的保存。

2. 安全设备

为了保证安全，企业网络中经常会加入一些安全设备，比如用于病毒防护的防毒墙、用于防止网络攻击的入侵检测系统和防火墙、用于远程安全连接的 VPN 设备等。这些专业的安全设备，是安全管理系统中的重头戏，但是在使用时需要和完善的配置规则相结合。

3. 访问控制规则

为了保证网络安全，通常会将一些没有必要的流量在特定的网络位置屏蔽掉，这需要依靠访问控制来实现。几乎大部分设备都能够实现访问控制的配置，但是配置的规则却差异很大。访问配置规则不能盲目地从单个设备考虑，需要全局把握，统一规划。

4. 安全协议

数据在网络中传输时，很可能因为各种原因而出现被损坏、被窃取、被篡改的情况。所以必须要使用一些能够确保数据完整性、机密性、正确性的技术，比如 SSL 传输协议、IPSec 协议、SNMPv3 协议等。除此之外，很多协议都自带有安全认证、加密功能。

5. 日志记录与分析

通过日志记录可以分析计算机系统、软件程序的所有操作内容，通过分析可以从中获得具有安全隐患的操作和造成故障威胁的原因，通常很多网络会专门做一套日志记录服务器。

6. 漏洞检测分析

漏洞是造成安全威胁的主要原因之一，一个小小的漏洞可能引发网络攻击、病毒木马攻击等一系列的安全问题。漏洞不可能完全避免，所以需要经常对网络进行分析，查找漏洞。

7. 警报策略

警报用于向管理员提示网络设备、系统服务等的异常。这可以让管理员第一时间发现故障隐患和解决故障，可以极大地减少损失。

1.4 网络管理体系结构

网络管理技术发展过程中，为了应对需求，网络管理方式做了很多的调整和变化。为了方便区分，可以用不同的网络管理体系结构对其进行定义。下面详细介绍网络管理体系结构的概念及分类。

1.4.1 网络管理体系结构概念

网络管理体系结构主要由网络管理系统和管理代理组成。它规定了网络管理信息采集管理的方式，随着网络规模的扩大，网络管理技术的发展，已经先后产生了三种网络管理体系结构，分别是集中式网络管理体系结构、分层网络管理体系结构和分布式网络管理体系结构。

1.4.2 集中式网络管理体系结构

集中式网络管理体系结构是将所有被管理设备的管理信息集中到一台管理服务器上实施网络管理。

如图 1-1 所示为集中式网络管理体系结构的拓扑图。

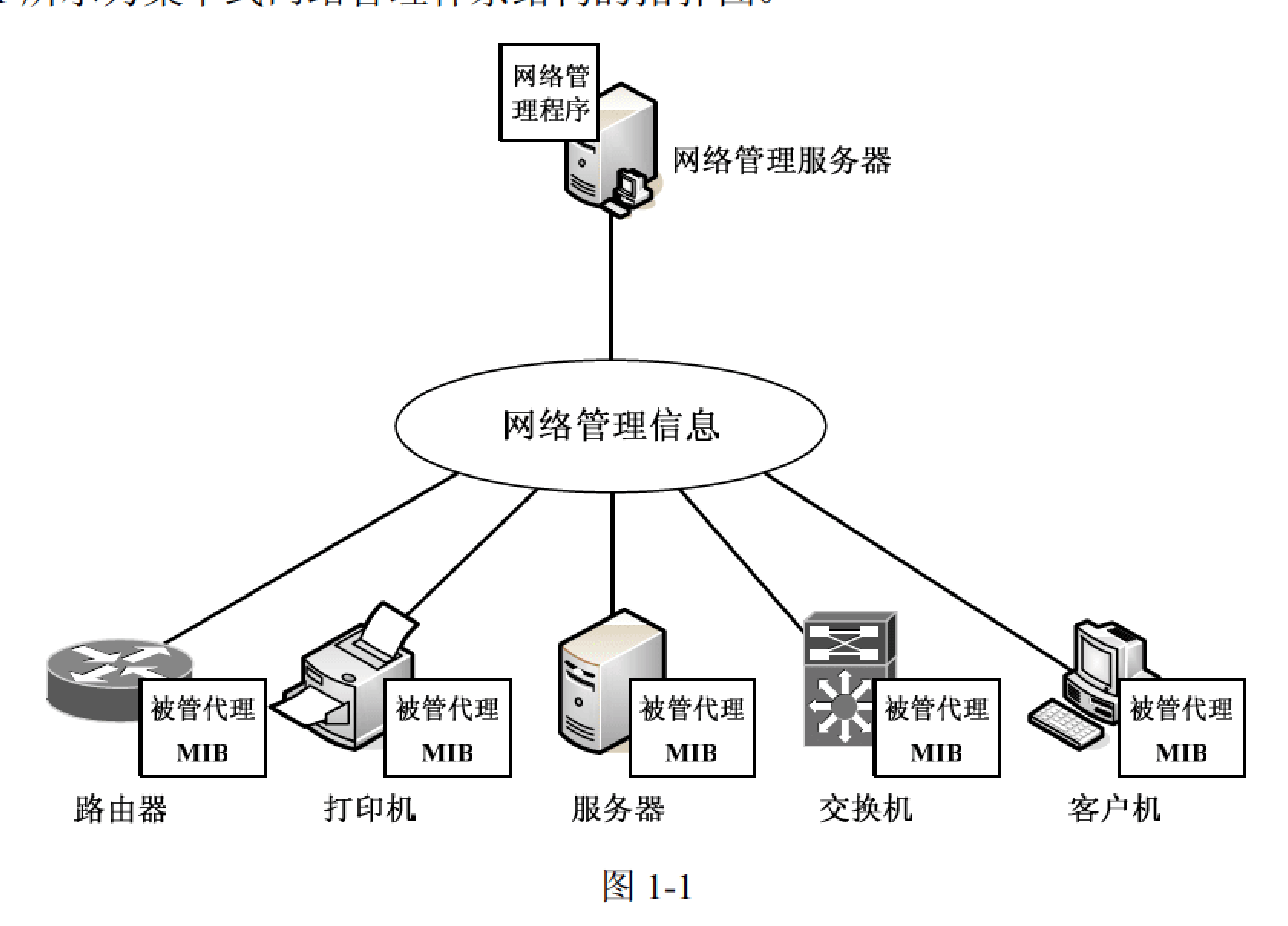


图 1-1

这种方式在早期网络管理中使用比较多。通过单一的网络管理服务器对全网进行监测、分析、维护和管理。集中式的管理方式不易出现管理上的冲突，但是随着网络管理任务量的增加，单个网络管理员根本应付不过来，单个网络管理服务器程序的性能也无法满足需求。

对于大型网络环境，虽然集中式网络管理体系结构已经不适用，但是大部分中小企业还是使用这种体系结构。

1.4.3　分层网络管理体系结构

继集中式网络管理体系结构之后就出现了分层网络管理体系结构。分层式网络管理体系加入了一层中间管理服务器，这个所谓的中间管理服务器并不能称作真正的服务器，而是被管设备上的一个内置管理程序，通过这个程序被管设备可以进行一些简单的网络管理任务，替网络管理服务器分担一些管理工作，缓解了整个网络的管理压力。

如图 1-2 所示为分层网络管理体系结构的拓扑图。

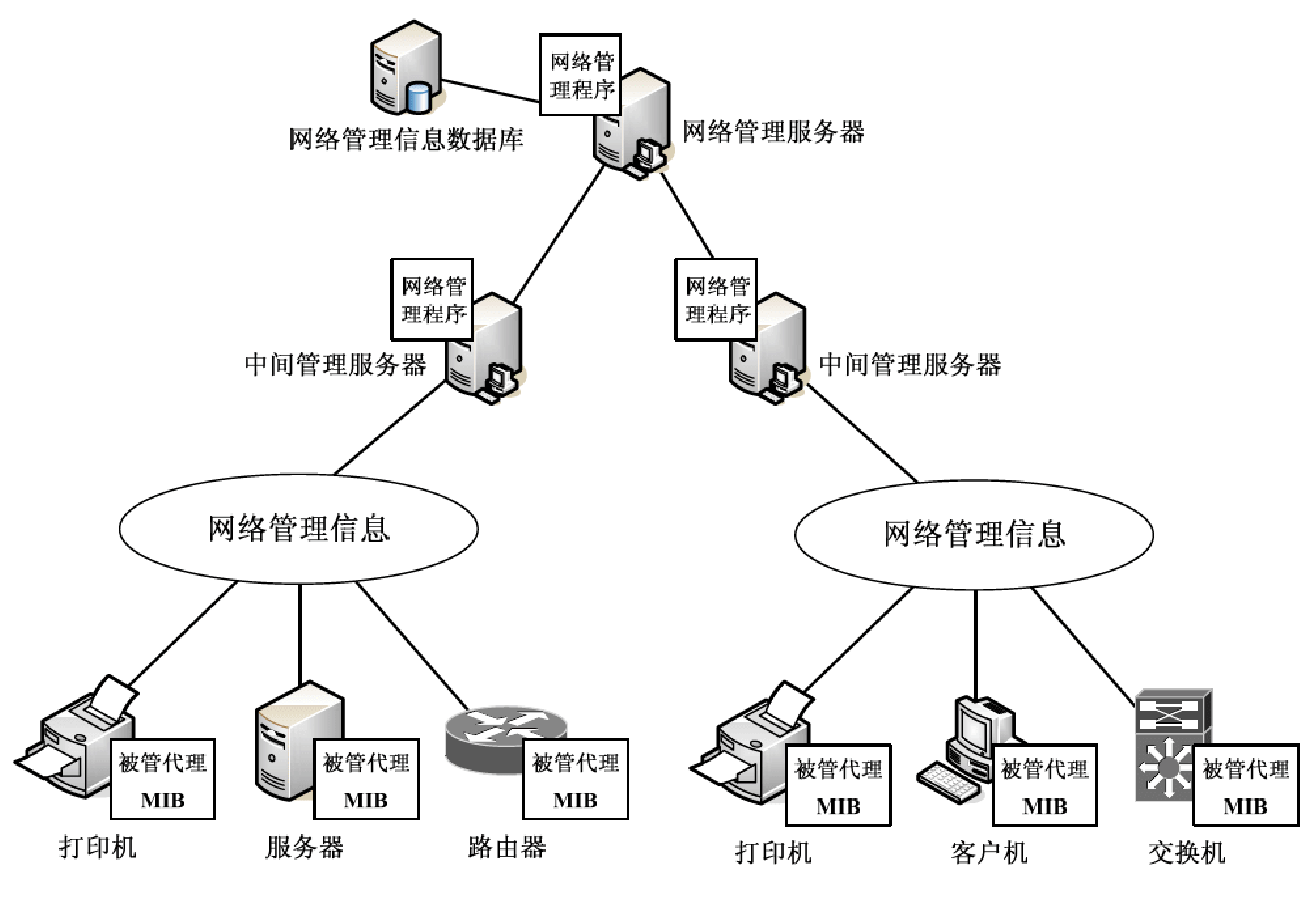


图 1-2

使用分层网络管理体系结构虽然做了管理工作的分散实施，但是整个网络管理体系还是只有一个管理信息数据库，被管设备和中间管理服务器没有信息存储能力。

1.4.4　分布式网络管理体系结构

企业在发展过程中业务类型越来越复杂，导致企业网络结构出现跨区域互联广泛、接入方式多等现象，所以需要更好的网络管理体系支持。

分布式网络管理体系结构可以说是对以上两种管理体系结构的整合与改进升级。将一个网络分配给多台服务器管理，每个服务器有一套网络管理程序和一个管理信息数据库，彻底分散了整个网络的管理任务。

如图 1-3 所示为分布式网络管理体系结构的拓扑图。

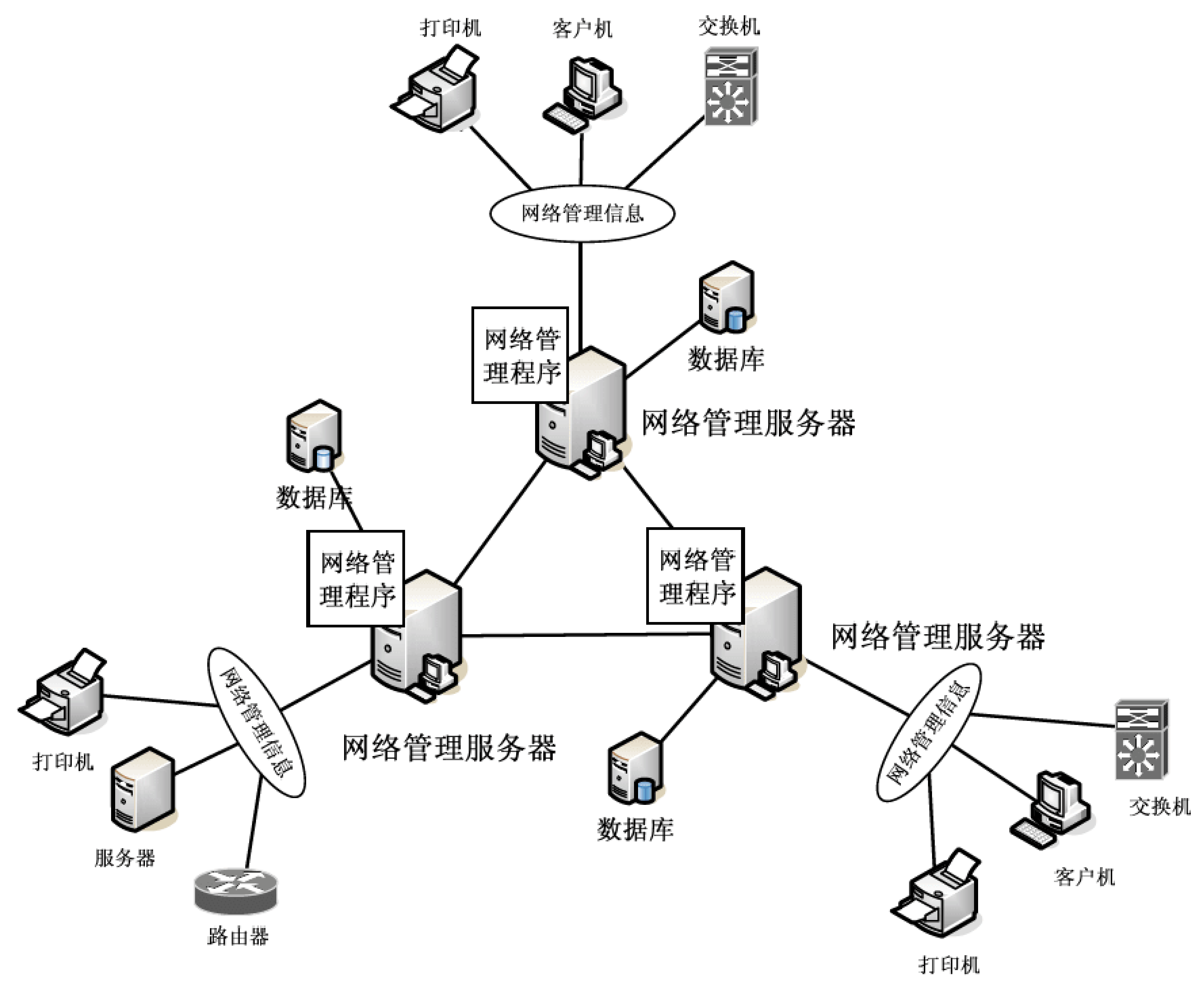


图 1-3

虽然网络环境进行了分散管理，但并不是一台服务器只能管理一个区域，如果需要获得其他区域的网络管理信息，服务器彼此之间可以相互访问获得。

1.5 网络管理实现模式分析

有了网络管理体系结构，如何在这种结构下获取网络管理信息呢？这就是下面要介绍的网络管理实现方式。常见的网络管理实现方式有：基于 SNMP 的网络管理、基于 CMIP 的网络管理、基于 Web 的网络管理、TMN 网络管理。

1.5.1 基于 SNMP 的网络管理

SNMP 协议是目前使用最多的网络管理协议，因为该协议是专门针对 TCP/IP 协议栈提出的，几乎所有互联网中应用的设备、服务器都支持 SNMP 协议。目前 SNMP 有三个版本 v1、v2 和 v3，使用比较广泛的是 v1 和 v2，但 v3 版本的安全性等多方面的性能都很高，所以未来一定是 v3 或更好的技术占领市场。

基于 SNMP 的网络管理系统包括四个要素：被管设备、被管设备中的管理代理、用于实现网络管理和监控功能的网络管理器、用于定义管理信息数据对象的 MIB（管理信息库）。

基于 SNMP 的网络管理系统主要通过四项工作来实现管理，介绍如下。

（1）管理服务器依靠 getrequest 和 getnetrequest 两种消息向被管设备代理发送信息请求，请求时主要依靠轮询的方式发送请求信息。

（2）被管设备代理使用 getresponse 消息对管理服务器的请求做出回复。

（3）管理服务器使用 setrequest 消息向被管设备代理发送管理信息修改请求。

（4）被管设备代理使用 trap 自陷消息主动向管理服务器报告被管设备中发生的事件。

1.5.2 基于 CMIP 的网络管理

CMIP 是 ISO（国际标准化组织）为了解决对不同厂商设备实施管理而创建的网络管理协议，是属于 OSI（开放式系统互连模型）体系的组成部分。

CMIP 和 SNMP 一样是一套完整的管理体系，在这个体系里有和 SNMP 网络管理体系一样的网络管理服务器、被管设备、被管设备代理和管理信息库四个要素。不过 CMIP 中的网络管理服务器和被管设备代理没有明确的区分，任何一台网络设备都可以同时担当这两个角色。CMIP 主要是通过事件报告进行工作的。

CMIP 网络管理体系主要由三部分组成。

（1）组织模型：规定了网络管理任务的分配

（2）功能模型：功能上可以分为故障管理、配置管理、性能管理、计费管理和安全管理五个部分。

（3）信息模型：面向所有管理功能都做了详细的 MIB 对象设计，但是 MIB 过于复杂了。

CMIP 也存在很多的优点，它可以在发送的每一个变量信息中携带一定的网络管理任务，减轻了网络管理员的工作和网络负担，同时 CMIP 还有较强的验证和访问控制功能。但是在实际应用时 CMIP 也存在很多问题，首先整个管理模型的使用会消耗掉 SNMP 几十倍的资源，每一个变量信息携带的管理任务都会增加被管代理的资源消耗，同时 CMIP 的 MIB 管理信息库设置过于复杂，不便于信息的查询和索引。

1.5.3 基于 Web 的网络管理

网络管理实现技术从 C/S（客户端/服务器）模式发展到了 B/S（浏览器/服务器）模式，使得整个 Web 技术搭建的环境有良好的可扩展性、开放性和可移植性，对于减少网络管理费用、提高网络管理效率等方面有极大的帮助，所有很多厂商纷纷开始投入到 Web 管理模型的开发中。

基于 Web 的网络管理（Web-Based Management），也可以称作 WBM。WBM 技术存在很多优点，它将 HTTP、Java、Web 和浏览器等多种技术和网络管理技术进行了融合，实现了更灵活、更高效、更强大的网络管理体系，作为网络管理者不需要再建立专门的网络管理服务器，只要有 Web 浏览器，在任何位置都可以实现网络管理。而且使用 Web 浏览器方式的管理易学易用，非常适合广大网络管理员使用。

1.5.4 TMN 网络管理

TMN（电信管理网）是电信网络业务中实现的网络管理技术，是在 CMIP 的基础上建立起来

的。是为了解决电信网络日益增加的设备数量和网络复杂性而设计的，可以提供更好的客户服务质量和高可靠性的电信服务。

整个 TMN 电信管理网也遵循五大网络管理功能。

（1）性能管理：对电信网和电信设备进行性能采集、统计，并对采集到的性能数据进行分析，根据性能分析结果，对电信网实施必要的控制措施。

（2）故障管理：对电信网和电信设备进行故障监测、分析和处理，可以实现警报提示、故障定位和故障修复功能。

（3）配置管理：对电信网络中的设备进行配置查看、调试操作，以及对业务信息进行配置调试，如为客户办理业务开启和关闭。

（4）帐务管理：对电信网络中客户的网络使用情况进行测量，判断其业务流量和应当缴纳的费用。

（5）安全管理：对电信网和电信设备进行加密、认证、审计和用户权限设置等操作，确保客户安全的使用电信网络。

对于普通企业来说，不需要过多的了解 TMN 网络管理模型。

1.6　专家答疑

（1）认识了网络管理技术，但是在具体工程中如何实施呢？

答：首先需要选择合适的网络管理体系结构，目前大多数中小企业都可以使用分层网络管理体系结构，大型企业可以选择分布式网络管理体系结构。然后确定使用什么样的网络管理协议，企业里的大部分网络都是使用的 SNMP 协议。之后就要结合网络管理的五大智能分别部署网络管理任务。

（2）网络管理技术不断发展，如何在原有的网络管理体系上升级？

答：如果之前网络中已经有了网络管理环境，一般网络管理体系已经确定了，不需要做调整。而使用的网络管理协议，目前大部分网络都是使用的 SNMPv2，如果企业有需求或者条件，可以在升级改造时，尽量将设备升级为支持 SNMPv3 协议，以提供更安全的保障。新增的网络设备可能会有新的管理优势，需要管理员及时学习发现，并加以利用。

第 2 章　简单网络管理协议 SNMP

初学网络管理技术，很多读者会提出这样的问题：网络管理服务器如何管理网络中的众多设备呢？被管设备又如何将自己的设备配置及状态信息反馈给管理服务器呢？这必须要有一种协议技术来实现该功能，网络管理协议应运而生。

网络设备繁多，为了使网络环境具有较高的可管理性，需要各种网络设备运用相同的网络管理协议。目前被各大设备厂商所认可的网络管理协议主要是 SNMP 协议。想要高效地完成网络管理任务，首先需要掌握 SNMP 协议的运行原理及相关运用技术，下面主要对 SNMP 协议进行详细讲解。

2.1　SNMP 概述

SNMP 协议由一些列的协议组和规范组成，它提出了一套从网络环境下的设备中获取网络管理信息的方法，同时也提出了设备向网络管理服务器报告问题和错误的方法。为了更深入的了解 SNMP 协议，下面对其发展、特点及存在的问题进行详细的介绍。

2.1.1　SNMP 的发展历程

为了简化大型网络中设备的管理与数据获取，上世纪 90 年代 SNMP 协议应运而生。当时很多流行的网络管理软件都是使用 SNMP 服务简化网络管理和维护的，比如 HP 的 Open View、IBM 的 Tivoli NetView 等。短短的几年，SNMP 服务的优越性就被各大网络产品厂商所认可，纷纷在自己的路由器、集线器等各类网络设备中加入该技术。这项技术发展到现在，各种设备上都默认配置了 SNMP 服务，从普遍使用的路由器、交换机，到单个的打印机、扫描仪，无一例外。

SNMP 服务并非一出世就很完美，在网络管理技术发展的历程中，SNMP 服务也在不断的完善。最先出现的 SNMP 被称作 v1 版，之后又相继出现了 SNMPv2 和 v3 两个版本。

SNMPv2 诞生于 1996 年，与 v1 版相比做了如下改善。

（1）支持分布式管理

SNMPv1 使用的是单一的集中式管理模式，而 SNMPv2 支持分布式 / 分层式的网络管理结构。在 SNMPv2 管理模型中允许系统同时具有管理器和代理的功能，一方面它可以以代理身份接收上一级管理系统的命令，访问其本机信息，另一方面还可以提供它所负责的管理域中其他代理的信息摘要，并向上级管理系统发送 Trap 信息。

（2）改进管理信息结构

增加了很多 SNMPv1 没有的数据类型，除了拥有一个相当于 SNMPv1 的 MIB-II 外，还有一个支持分布式管理结构的 Manager-to-Manager（M2M）MIB。

（3）增强了管理信息通信协议的能力

增强了对大块数据的读取，并允许 Manager（管理站）间发送通报。随着技术的发展，安全的需求，2002 年 SNMPv3 诞生。由于使用 SNMPv1 和 v2 进行网络管理时安全功能有限，面临着假冒、信息篡改、信息暴露等多种安全威胁，在 SNMPv3 中增强了加密和验证功能，使其具有极好的安全性和管理功能。虽然功能有所增强，但是 SNMPv3 依然保留了 SNMPv1 和 v2 易于理解、易于实现的特点。

2.1.2　使用 SNMP 需要注意的问题

SNMP 协议得到了广泛应用，很多厂商都采用其协议标准，但是许多厂商依然使用 SNMPv1 和 v2，并没有使用安全性和管理功能更好的 SNMPv3。SNMPv1 和 v2 两个版本唯一的安全手段就是共同体名，没有过硬的安全加密技术。一旦获取了共同体名就可以连接设备获取想要的管理信息。为了方便管理，大多数设备会配置一个默认的共同体名，一般为 public（只读权限）和 private（读/写权限），如果管理员没有做修改，网络资源信息很容易被窃取。

SNMPv1 和 v2 版本大部分信息还是以明文进行传输，即便是做了加密也很容易被截获，破解出共同体名。

SNMPv3 虽然做了很多安全技术，但是如果应用不好，默认的共同体名依然会造成其安全隐患。

除此之外，很多设备在出现异常时会向管理服务器提交 SNMP Trap（陷阱）信息，这些信息主要是异常报告，信息中除了异常原因、现象外还有重要的设备系统、状态信息。信息一旦被攻击者获得，会对网络造成很大的威胁。

2.2　SNMP 管理系统

在实施网络管理时，构成了一套由五部分构成的网络管理系统。这 5 部分分别是：被管设备、管理代理、网络管理器、网络管理协议和管理信息库。

（1）被管设备（Managed Devices）：被网络管理员监控管理的设备。

（2）管理代理（Agent）：这是驻留在被管设备中的软件程序，主要用于获得被管设备的硬件信息、系统配置、运行状态等信息。一般代理程序都是设备出厂设置的。

（3）网络管理器（Network Manager）：用于管理、监控其他设备的管理服务器。

（4）网络管理协议（Network Management Protocol）：提供了一种从网络上的设备中收集网络管理信息的方法。

（5）管理信息库（Management Information Base，MIB）：MIB 是一个信息存储库，定义了数千个数据对象。网络管理员可以通过控制这些数据对象来完成网络设备的控制、监控和配置。

SNMPv3 可以实现分层的网络管理模型，一般整个网络管理系统需要有一个网络管理服务器、

几个中间管理服务器、多个被管设备、和一个或多个 MIB 管理信息库。图 2-1 给出一个多层次的网络管理系统模型。

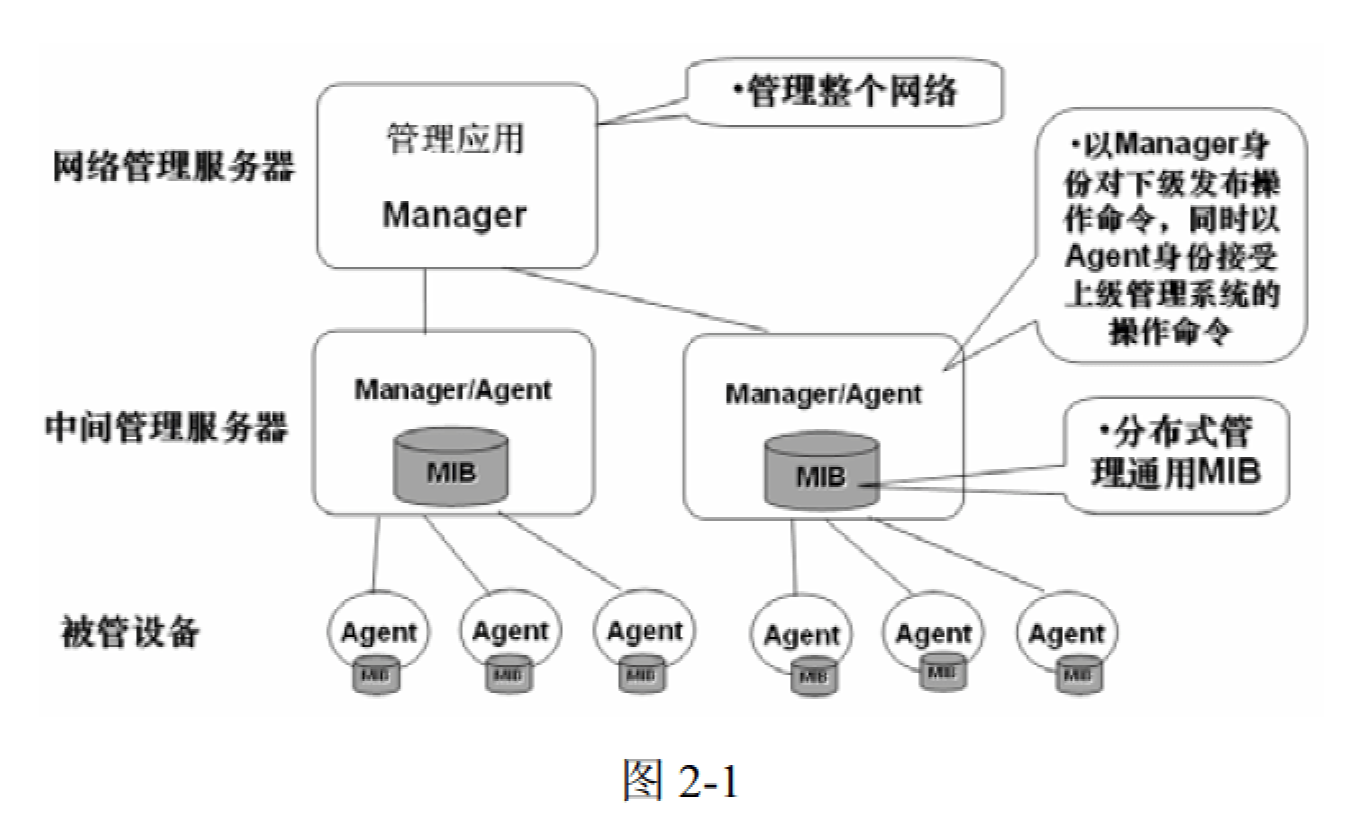


图 2-1

2.3 SNMP 实现机制

SNMP 网络管理系统构成后，如何实现工作呢？这主要通过以下四项工作来实现。

（1）管理服务器向被管设备的代理提出询问消息，以获取指定信息。
（2）代理接收到管理服务器的询问之后，自动应答消息。
（3）代理主动地向管理服务器提供有关被管设备性能、状态、错误等的自陷消息。
（4）管理服务器使用基于轮询和中断的方式实时进行被管设备的信息收集。

总结以上四项工作内容，SNMP 的实现机制一共产生了五种消息，分别是：getrequest、getnetrequest、setrequest、getresponse 和 trap。用图形来表示管理服务器和代理程序之间的这五种消息，可构成如图 2-2 所示的网络管理框架。

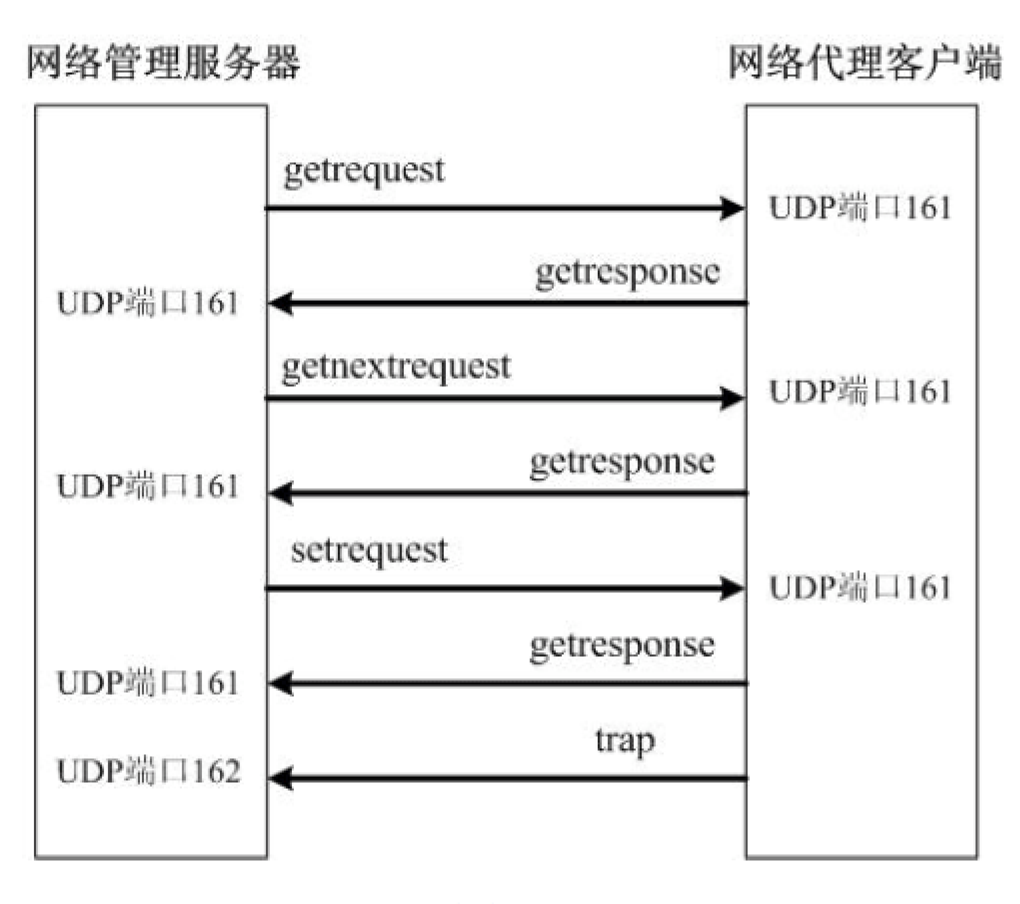


图 2-2

各种消息的意义如下。

（1）getrequest：用于向被管设备的代理请求提取网管信息。

（2）getnetrequest：请求读取从被管设备提取的管理信息。

（3）setrequest：请求修改或设置被管设备的管理信息。

（4）getresponse：对各种读取和修改管理信息的请求进行应答。

（5）trap：主动向管理服务器报告被管设备中发生的事件。



SNMP 协议主要使用的是 UDP 协议的 161 和 162 端口，其中只有 trap 信息使用的是 162 端口，其他都是 161 端口。在使用网络安全设备进行端口过滤时判定是否有 SNMP 流量需要通过，如有需要，要单独指定该流量通过安全设备。

确定了 SNMP 网络管理协议实现网络管理时的几种消息，还需要了解网络管理服务器是如何发送请求收集数据的。这主要依靠三种方式来实现，分别是轮询、中断和面向自陷的轮询。

（1）轮询（polling）：网络管理服务器会一次向所有被管设备代理发送 getrequest 消息，询问完最后一个设备后，会从第一个设备继续发送 getrequest 消息。通过这种不断循环的询问方式实时的获取被管设备的管理信息。但是这种方式获取的实时信息，往往会出现错误的实时性，轮询方式如图 2-3 所示。

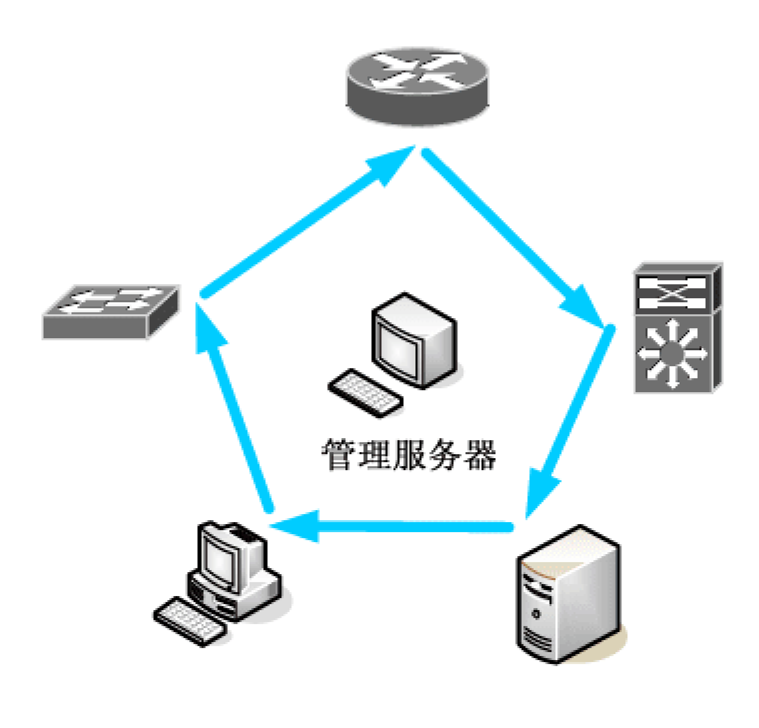


图 2-3

（2）中断（Interrupt）：被管设备代理在发现设备异常事件时，主动向管理服务器发送自陷信息。如果被管设备的代理不主动发送，网络管理服务器无法获取被管设备信息，中断方式如图 2-4 所示。

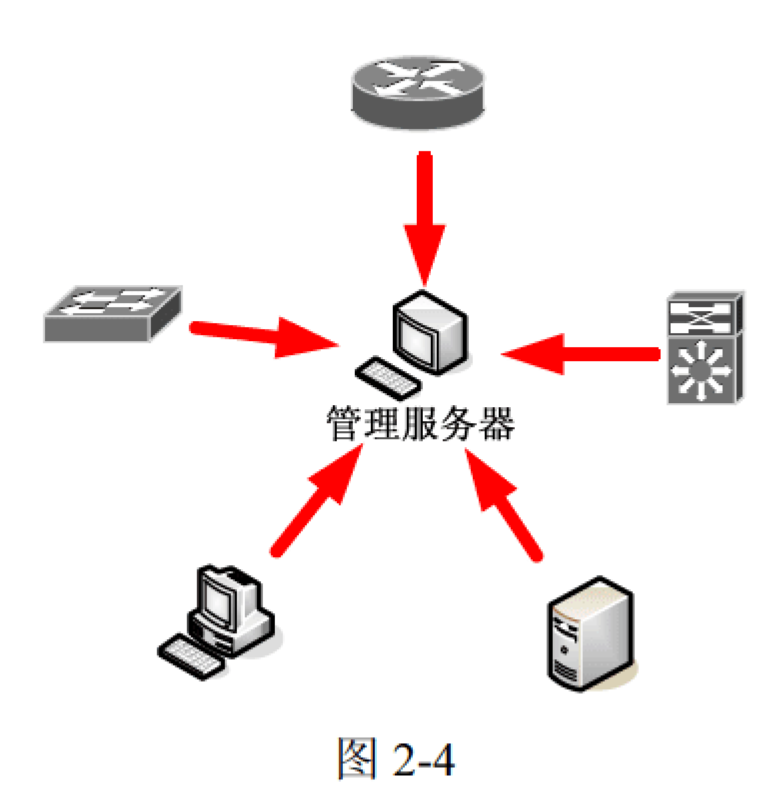


图 2-4

（3）面向自陷的轮询（trap-directed polling）：单一的使用轮询或者中断都存在管理上的缺陷，所以一般建议采取两者结合的方式实施网络管理，如图 2-5 所示。

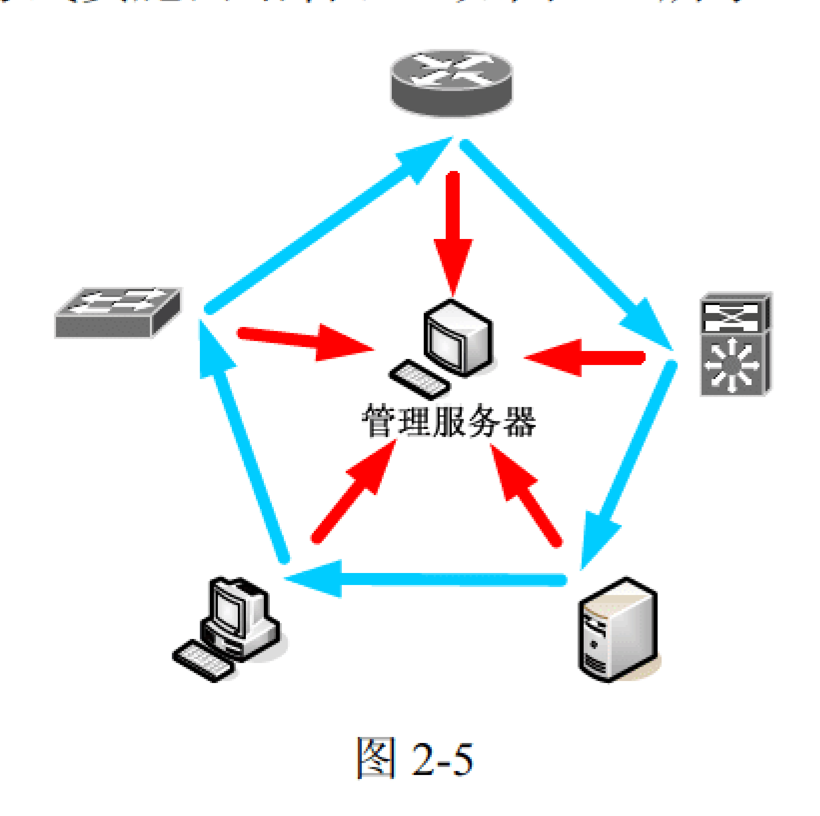


图 2-5

2.4　SNMP 安全分析与安全机制

在 SNMP 协议中确保安全的机制之一就是 community string（共同体），所谓 community string 是 SNMP 管理服务器和代理之间进行身份认证的一个口令。管理服务器在向代理发送请求信息时会带着自身指定的共同体名一起发送，被管设备代理接收到请求信息，会与自身设置的共同体名进行比较，如果两个共同体名一致，则进行消息应答，否则丢弃 SNMP 管理请求信息。共同体名认证原理可以用图 2-6 来表示。

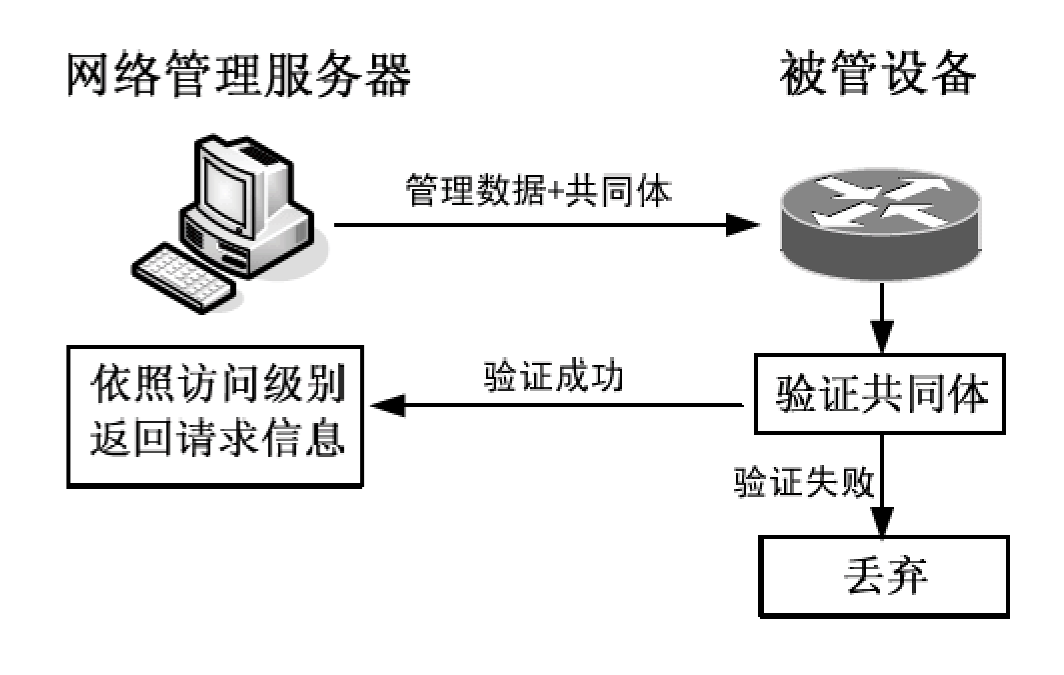


图 2-6

SNMP 共同体的作用可以总结为以下三点。

（1）认证服务：可以指定被授权的管理服务器才有访问被管设备管理信息的权限。

（2）访问策略：对不同的管理服务器可以设定不同的管理级别，以实现分层多级网络管理。

（3）代理服务：可用于中间管理服务器以代理身份提供认证服务和访问策略，限制上级管理服务器对下级被管设备的管理。

由于很多设备都设置了默认的共同体名，所以网络管理会存在安全隐患。在架设网络管理系统时一定要使用具有较高安全性的共同体名。

2.5　配置 SNMP 网络管理协议

网络环境中的设备种类比较多，想要对所有设备进行管理，必须要先开启这些设备的 SNMP 网络管理协议，下面主要对 Windows、Linux、Cisco 路由器三种常见设备的 SNMP 协议开启、配置方法进行介绍。

2.5.1　开启 windows 的 SNMP 协议

安装 Windows 操作系统的主机在网络中使用的比例比较大，常见的有 Windows XP、Windows Server 2003、Windows Server 2008、Windows 7 等，但是无论哪一个版本的 Windows 系统其安装、配置 SNMP 的方法都是相似的。下面以 Windows Server 2003 为例进行介绍。

1. 安装 SNMP 组件

大部分的 Windows 操作系统是没有安装 SNMP 组件的，所以首先要进行 SNMP 的组件安装，具体操作步骤如下。

01 单击【开始】按钮，在弹出的菜单中选择【设置】➢【控制面板】菜单命令，如图 2-7 所示。



图 2-7

02 弹出【控制面板】窗口，选择【添加或删除程序】选项，如图 2-8 所示。



图 2-8

03 弹出【添加或删除程序】窗口，在左侧的列表中选择【添加/删除 windows 组件】选项，如图 2-9 所示。



图 2-9

04 弹出【Windows 组件向导】对话框，在【组件】选项列表中双击【管理和监视工具】选项，如图 2-10 所示。



图 2-10

05 弹出【管理和监视工具】对话框，选择【简单网络管理协议（SNMP）】复选框，单击【确定】按钮，如图 2-11 所示。

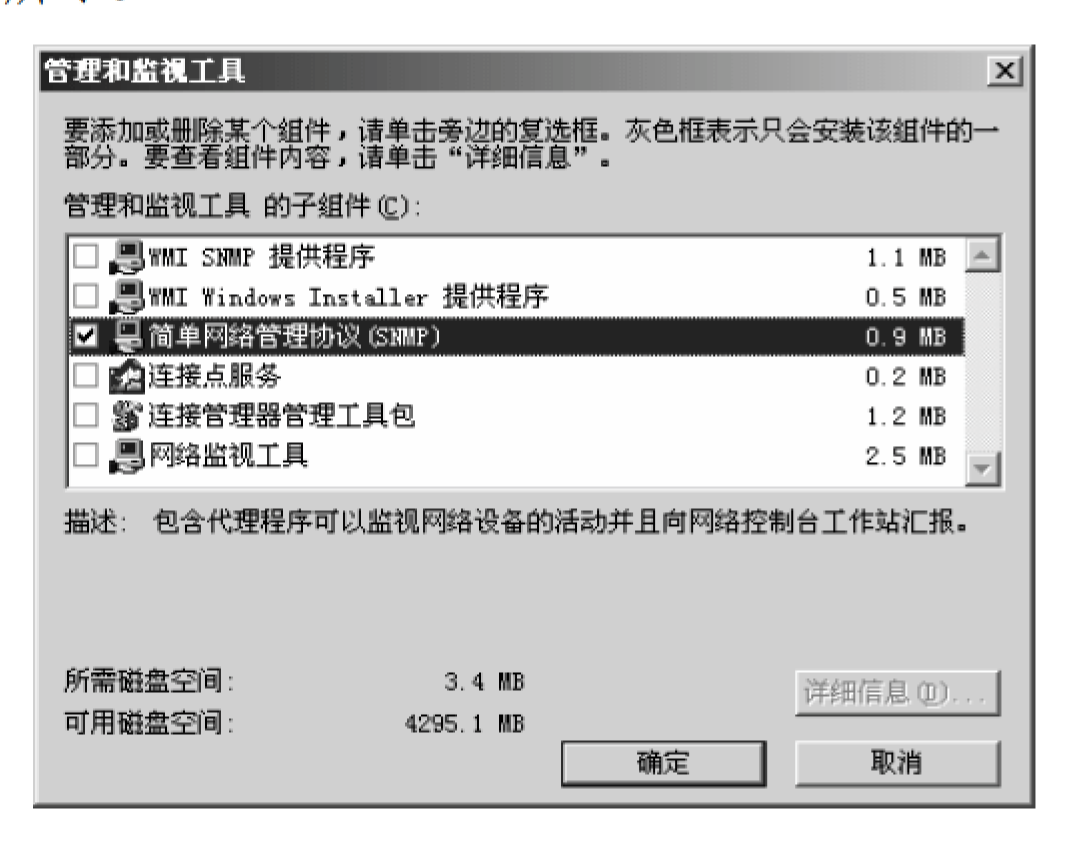


图 2-11

06 返回【Windows 组件向导】对话框，【管理和监视工具】选项已被勾选，单击【下一步】按钮，如图 2-12 所示。

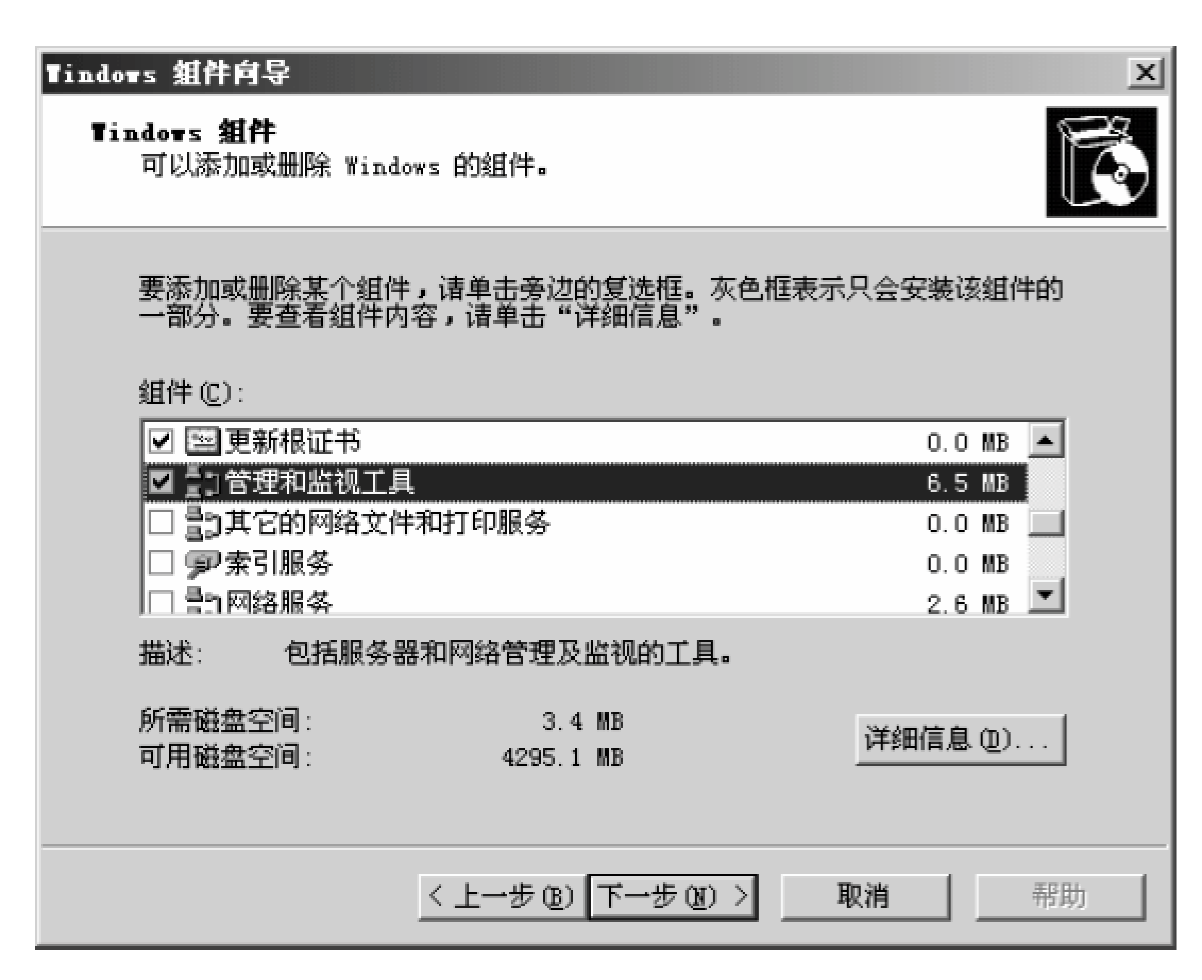


图 2-12

07 系统自动安装已选组件，并显示安装进度，如图 2-13 所示。



图 2-13

08 组件安装完成后，单击【完成】按钮，如图 2-14 所示。



图 2-14

2. 配置 SNMP 服务项

安装 SNMP 组件后，默认可以直接使用，但是不同的网络管理环境要求或管理参数配置不尽相同，所以在使用之前，首先要保证 SNMP 服务的正确可用。

配置 SNMP 服务的具体操作步骤如下。

01 单击【开始】按钮，在弹出的菜单中选择【运行】菜单命令。弹出【运行】对话框，在【打开】文本框中输入"services.msc"命令，单击【确定】按钮，如图 2-15 所示。



图 2-15

02 弹出【服务】窗口，在右侧系统服务列表中可以找到【SNMP Service】（SNMP 服务）和【SNMP Trap Service】（SNMP 陷阱）服务项，两个服务均处于【已启动】状态，说明当前主机的 SNMP 服务可用，双击【SNMP Service】（SNMP 服务）服务项，如图 2-16 所示。



图 2-16

03 弹出【SNMP Service 的属性（本地计算机）】对话框，选择【陷阱】选项卡，如图 2-17 所示。

SNMP Service 的属性(本地计算机)
常规 登录 恢复 代理 陷阱 安全 依存关系
服务名称: SNMP
显示名称(N): SNMP Service
描述(D): 使简单网络管理协议(SNMP)请求能在此计算机上被处理。如果此服务停止，计算机将不能处理 SNMP 请求。如果此服务被禁用，所有明确
可执行文件的路径(H):
C:\WINDOWS\System32\snmp.exe
启动类型(E): 自动
服务状态: 已启动
启动(S) 停止(T) 暂停(P) 恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定 取消 应用(A)

图 2-17

04 当主机出现异常时，可以通过陷阱服务将异常现象主动反馈给 SNMP 管理服务器，在【团体名称】文本框中输入有效团体名，本实例采用默认值“public”，单击【添加】按钮，如图 2-18

所示。

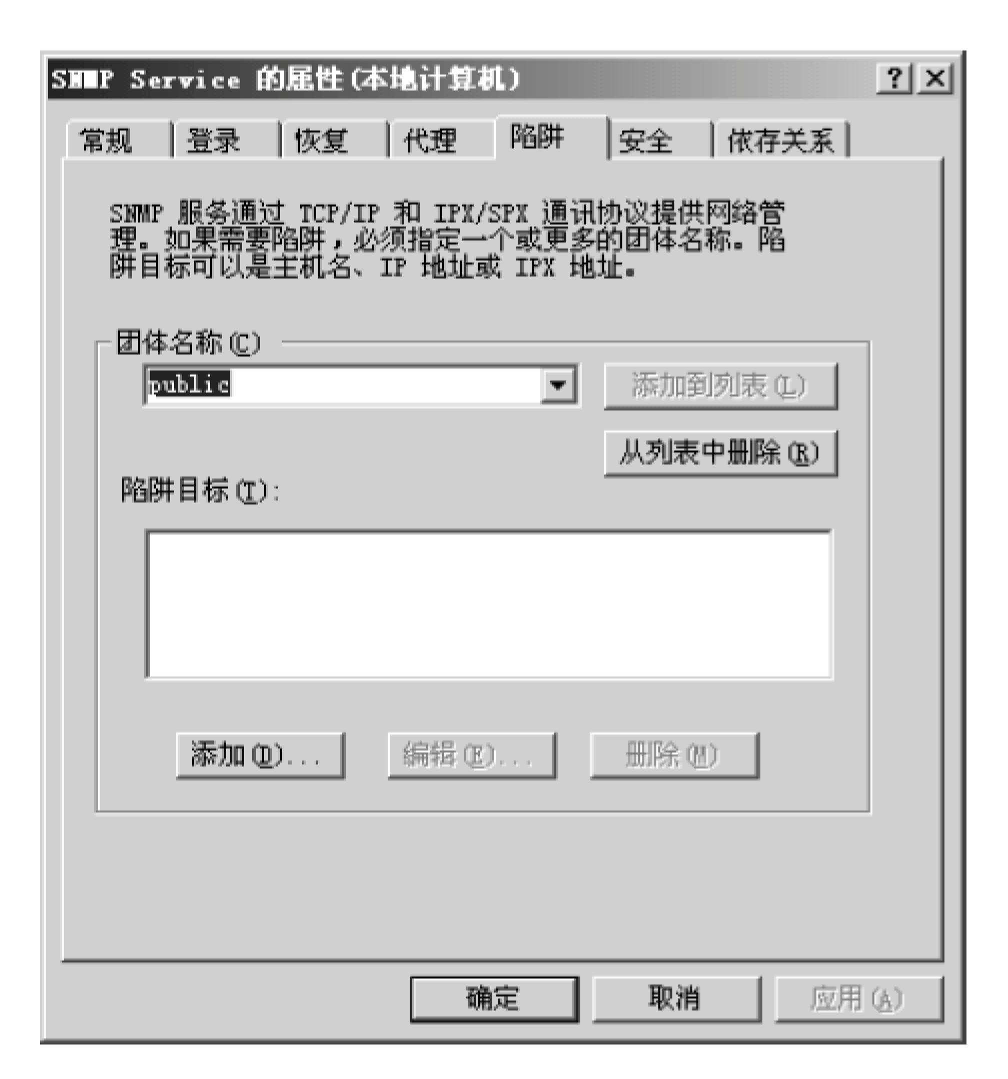


图 2-18

05 弹出【SNMP 服务配置】对话框，在【主机名，IP 或 IPX 地址】文本框中输入陷阱目标主机地址，一般为网络管理服务器的主机地址，单击【添加】按钮，如图 2-19 所示。



图 2-19

06 返回【陷阱】选项卡，在【陷阱目标】列表中显示新添加的陷阱目标主机地址，如图 2-20 所示。

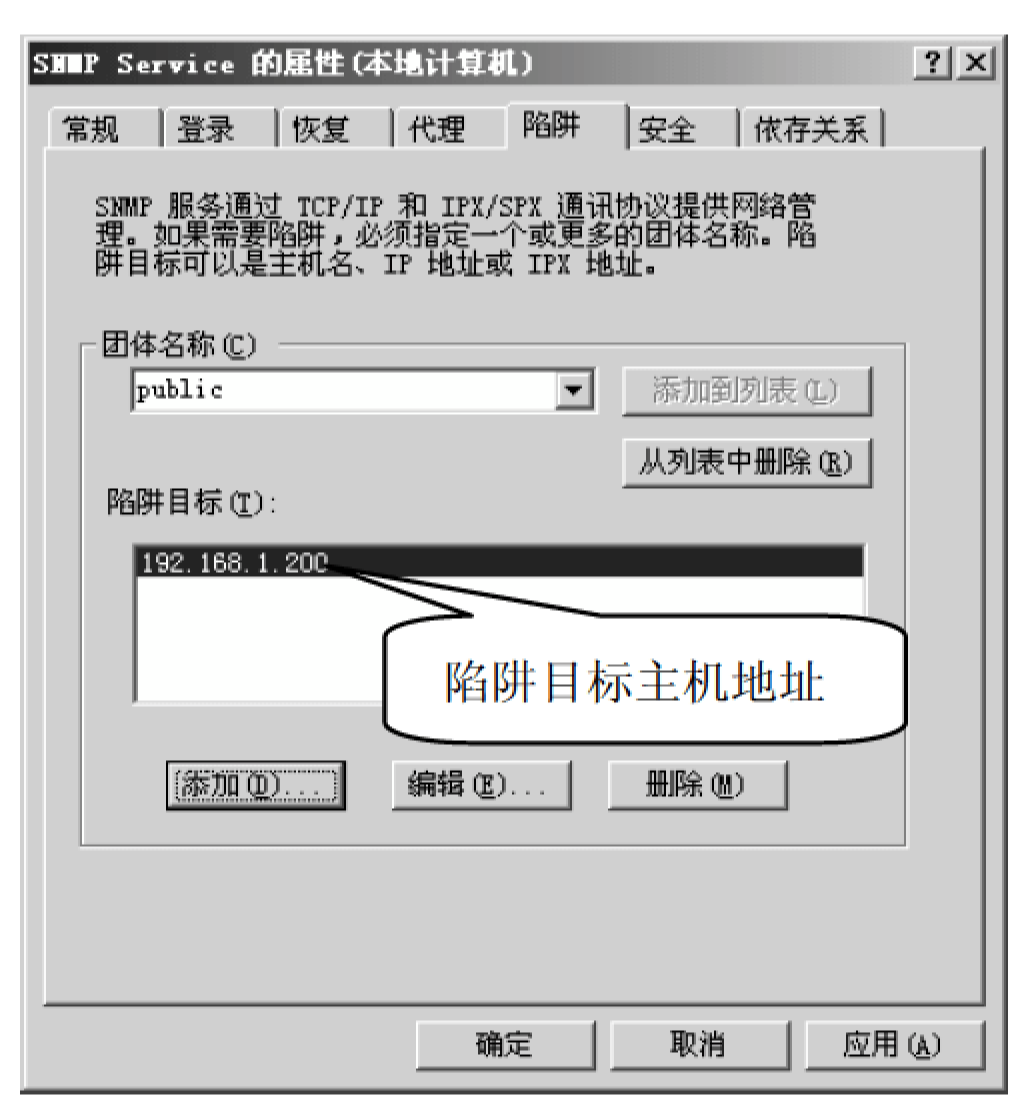


图 2-20

07 选择【安全】选项卡，在【接受团体名称】窗格中显示了可用团体名，默认团体名为“pubic”，权限为“读写”，单击【添加】按钮，如图 2-21 所示。

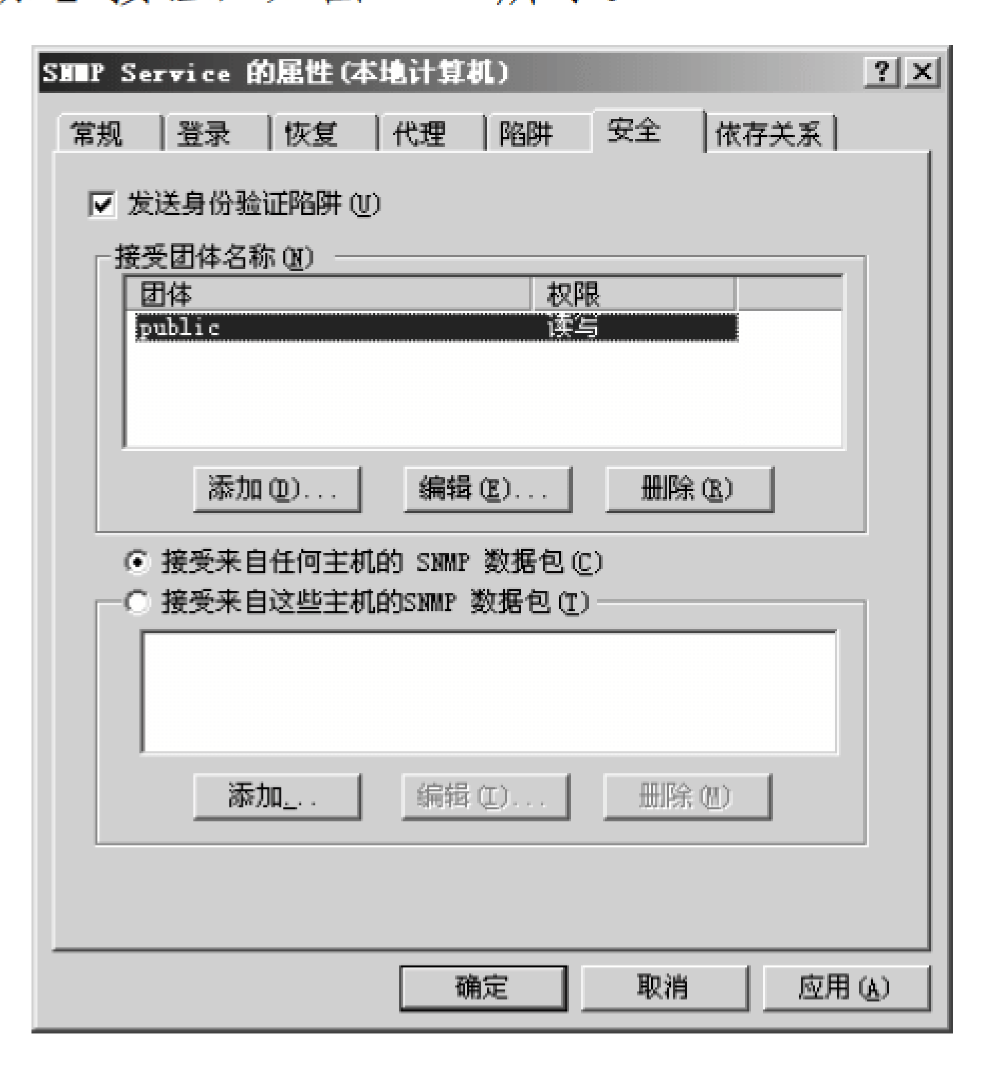


图 2-21

08 弹出【SNMP 服务配置】对话框，在【团体名称】文本框中可以输入新的可用团体名，如图 2-22 所示。

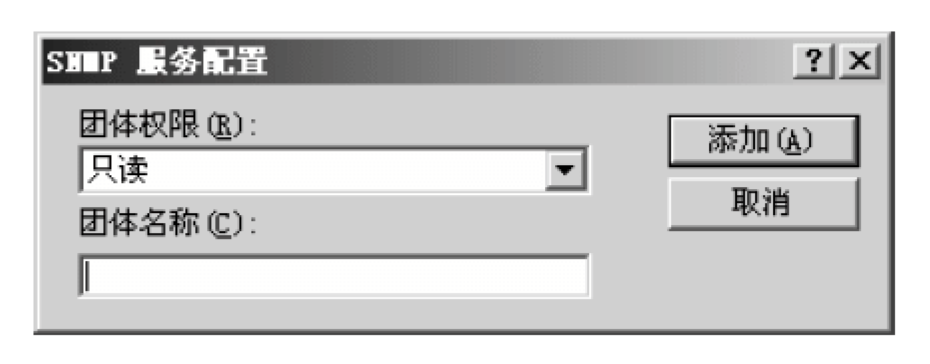


图 2-22

09 打开【团体权限】下拉菜单，可以设定对应团体名的权限，可以根据实际需求进行选择，单击【确定】按钮，如图 2-23 所示。



图 2-23

10 返回【安全】选项卡，本实例添加了一个团体名为“SMNP”，权限为“只读”的接受团体名称，单击【确定】按钮，完成 SNMP 服务的设置，如图 2-24 所示。

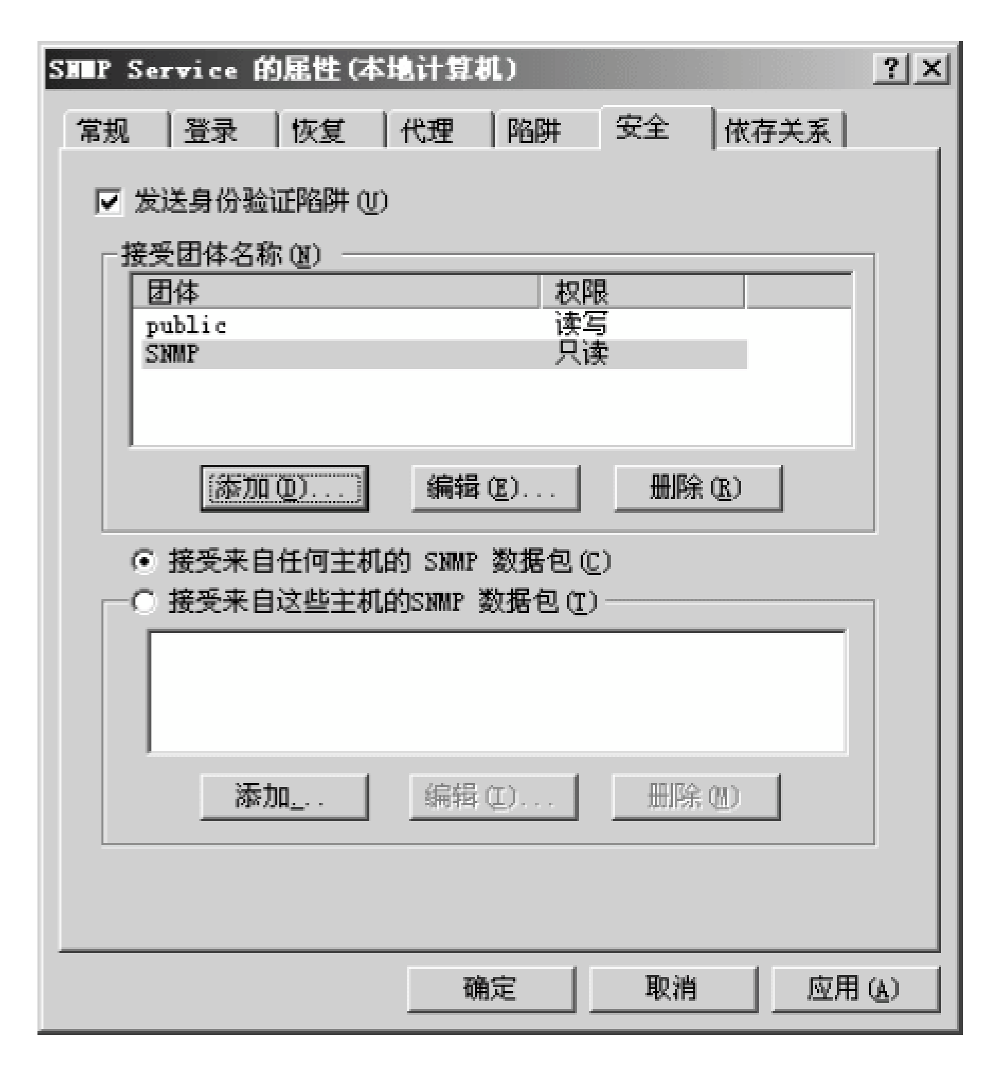


图 2-24

2.5.2 开启 Linux 的 SNMP 协议

Linux 系统的版本比较多，很多系统默认没有安装 SNMP 软件包，需要进行手动安装。SNMP 软件包比较小，本实例采用 RPM 包安装方法，下面介绍其具体的安装与配置方法。

1. 安装 SNMP 软件包

SNMP 主要需要安装两个包分别是 net-snmp-libs 和 net-snmp，将软件包下载到/root 目录，运行 RPM 命令进行安装，具体配置命令如下。

```
[root@localhost ~]#rpm –ivh Net-snmp-libs-5.1.2-11
[root@localhost ~]#rpm –ivh net-snmp-5.1.2-11
```

查看软件包是否安装成功。

```
[root@localhost ~]# rpm –qa |grep snmp
net-snmp-libs-5.1.2-11
net-snmp-5.1.2-11
```

2. 配置 SNMP 服务

安装好后需要对 mib 支持和 community string（共同体）进行设置，默认 SNMP 主配置文件为/etc/snmp/snmpd.conf，具体配置命令如下。

```
[root@localhost ~]#vi /etc/snmp/snmpd.conf
```

打开配置文件后需要做以下几点配置。

（1）修改 community string

在配置文件 41 行可以设定默认的 community string 值，将 public 改为更安全的口令。

```
41 Com2sec notConfigUser default public
```

（2）修改管理信息库

在配置文件 62 行可以修改默认使用的管理信息库，将该行的 systemview 修改为 mib2，并确保 88 行前面的#号去掉。

```
62 Access notConfigGroup any noauth exact s mib2 none none
……
88 View mib2 included .iso.org.dod.internet.mgmt.mib-2 fc
```

（3）重启 SNMP 服务

配置结束后必须重启服务才可生效。SNMP 程序的服务名为 snmpd，可以使用以下两种方法重启该服务。

```
[root@localhost ~]#/etc/init.d/snmpd testart
```

或

```
[root@localhost ~]#Service snmpd restart
```

2.5.3 开启网络设备的 SNMP 协议

以思科路由器为例配置 SNMP 协议，具体配置命令如下。

```
Router(config)#snmp-server community howin rw
//配置本路由器的读写字串为 howin
Router(config)#snmp-server community howin ro
//配置本路由器的只读字串为 howin
Router(config)#snmp-server enable traps
//允许路由器将所有类型 SNMP Trap 发送出去
Router(config)#snmp-server host IP_SERVER traps howin
//指定路由器 SNMP Trap 的接收者，发送 Trap 时采用 howin 作为字串
Router(config)# snmp-server trap-source loopback0
//将 loopback 接口的 IP 地址作为 SNMP Trap 的发送源地址，注意先配好 IP 地址
```

2.6 典型 SNMP 网络管理案例

前面对 SNMP 网络管理协议做了系统介绍，为了更直观的看到 SNMP 网络管理协议的用途，下面列举一个简单的例子。

本案例采用 Snmputil 工具来实现网络管理，snmputil.exe 是命令行下的工具，要在命令行下才能运行，具体调用 snmputil.exe 的操作步骤如下。

01 将下载到的 Snmputil 工具放在 C 盘根目录下，单击【开始】按钮，在弹出的菜单中选择【运行】菜单命令。弹出【运行】对话框，在【打开】文本框中输入“cmd”命令，单击【确定】按钮，如图 2-25 所示。



图 2-25

02 弹出命令提示符窗口，输入“C: ”，按【Enter】键确认，如图 2-26 所示。

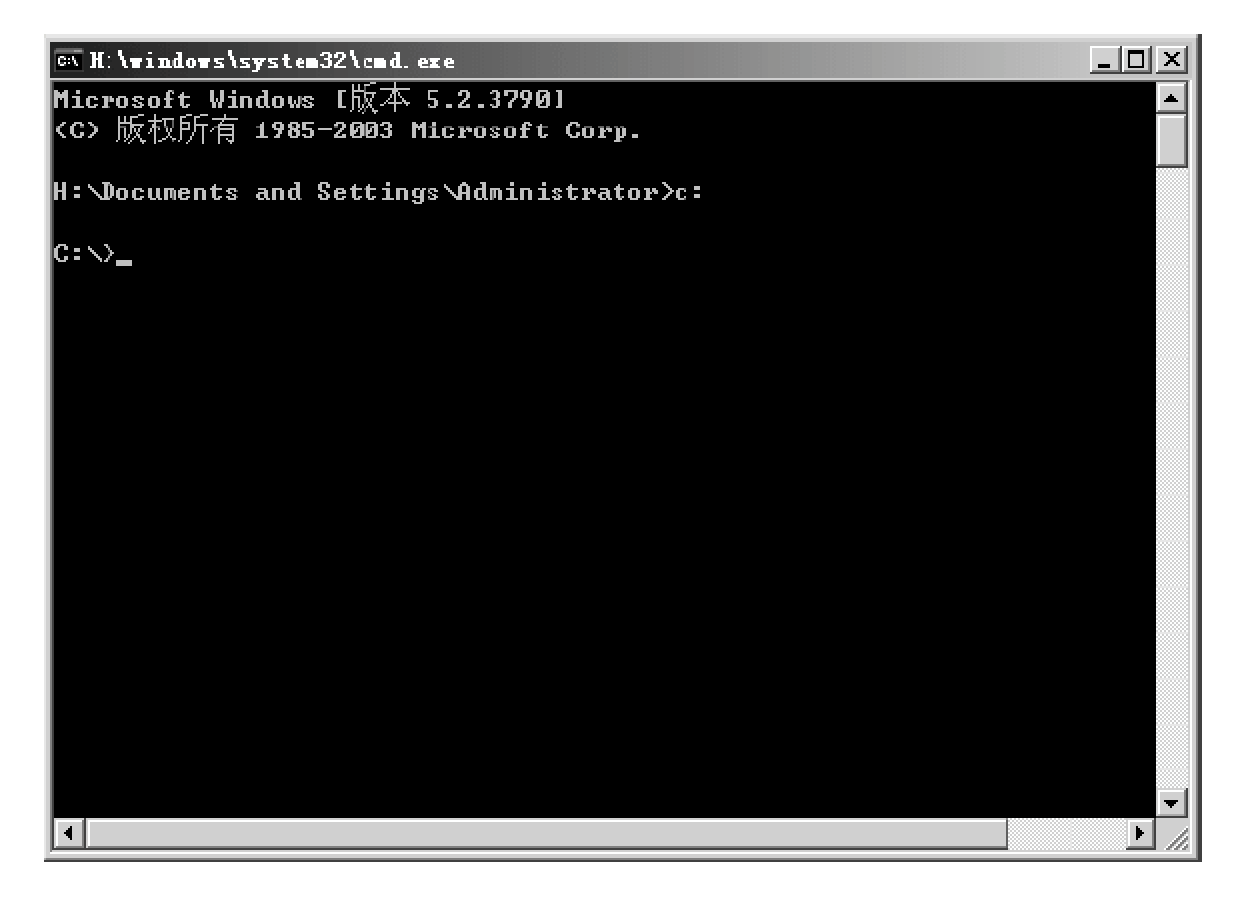


图 2-26



如果 Snmputil 工具没有放在盘符的根目录下，例如放在 C 盘下的 Snmputil 文件夹下，需要进入 Snmputil 文件夹下，命令为“cd Snmputil”，如图 2-27 所示。

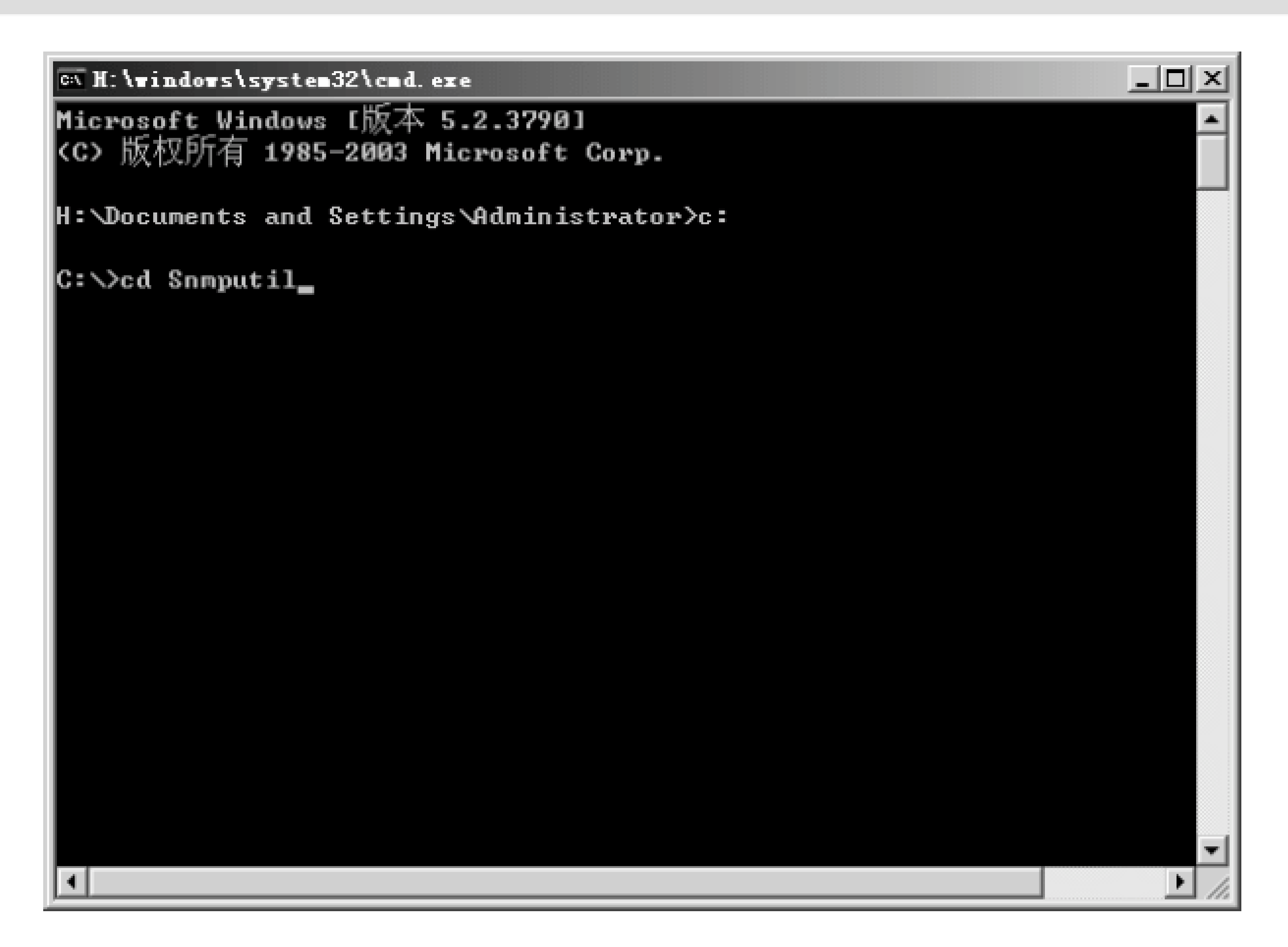


图 2-27

03 输入“snmputil.exe”，按【Enter】键确认，即可调用 Snmputil 工具，如图 2-28 所示。

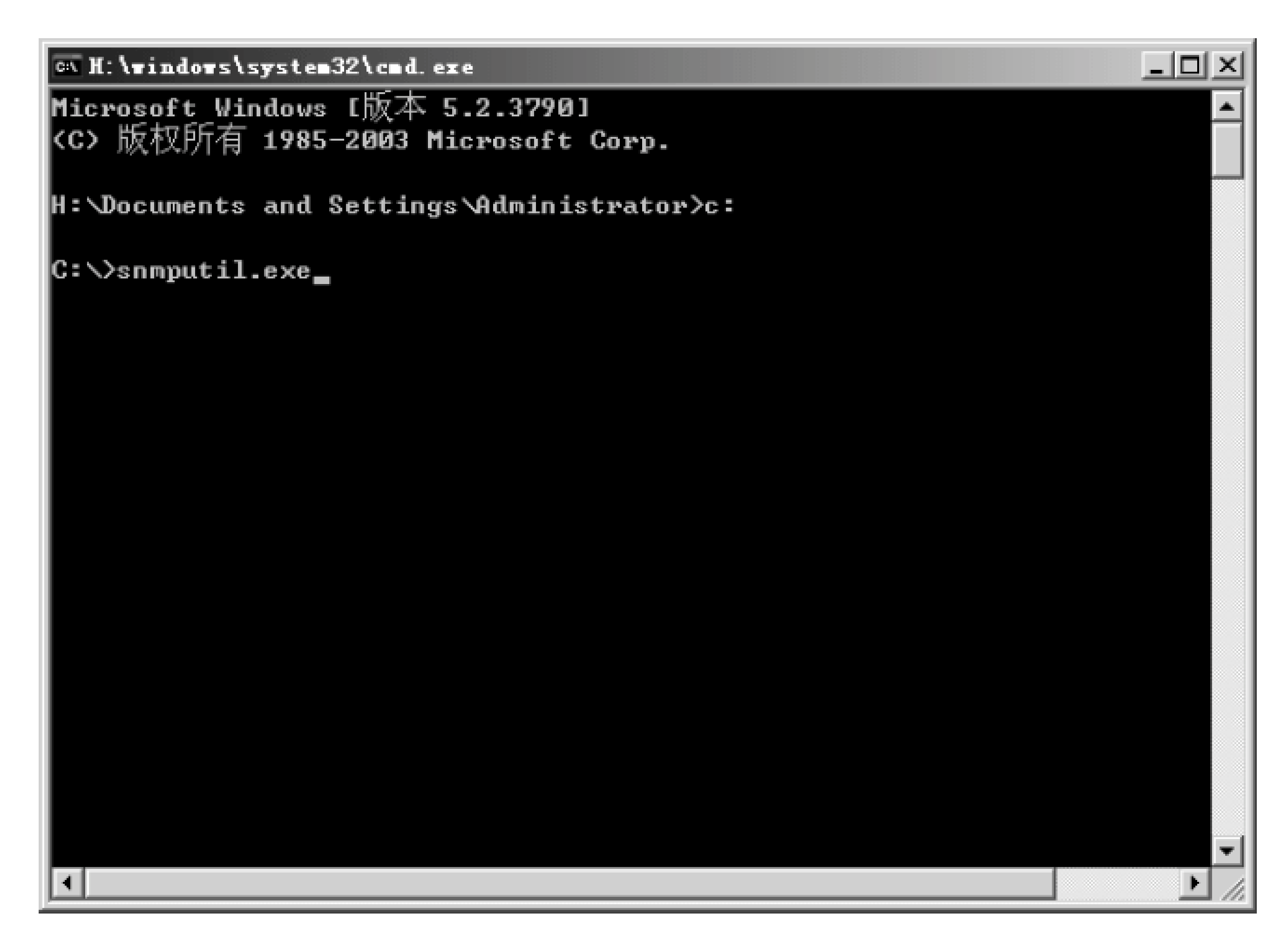


图 2-28

Snmputil 工具通过指定的 MIB 标识符查看被管设备的管理信息，下面案例中会列举 5 个常用 MIB 管理对象的标识符。在网络管理服务器和被管设备上安装 SNMP 程序，并采用默认的共同体名“public”。

假设被管理设备的 IP 地址为 192.168.1.104，使用 Snmputil 工具查看被管理设备信息的具体操作步骤如下。

01 输入命令“snmputil.exe walk 192.168.1.104 public .1.3.6.1.2.1.25.4.2.1.2”，按【Enter】键确认，即可显示设备的当前进程列表，如图 2-29 所示。

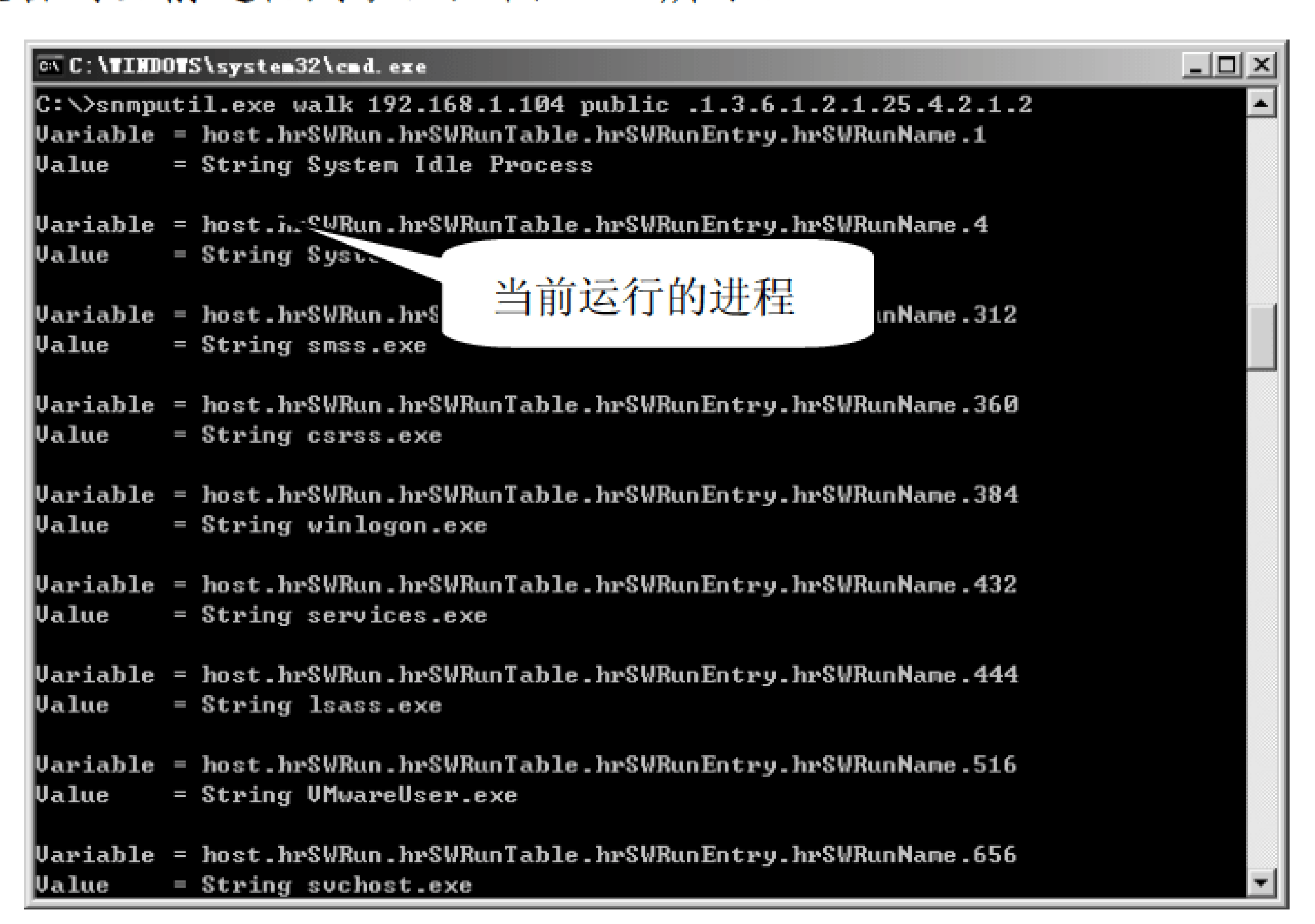


图 2-29



在图 2-29 中，【value】参数后显示的是查询的管理信息。

02 输入命令“snmputil walk 192.168.1.104 public .1.3.6.1.4.1.77.1.2.25.1”，按【Enter】键确认，即可显示设备的系统用户列表，如图 2-30 所示。

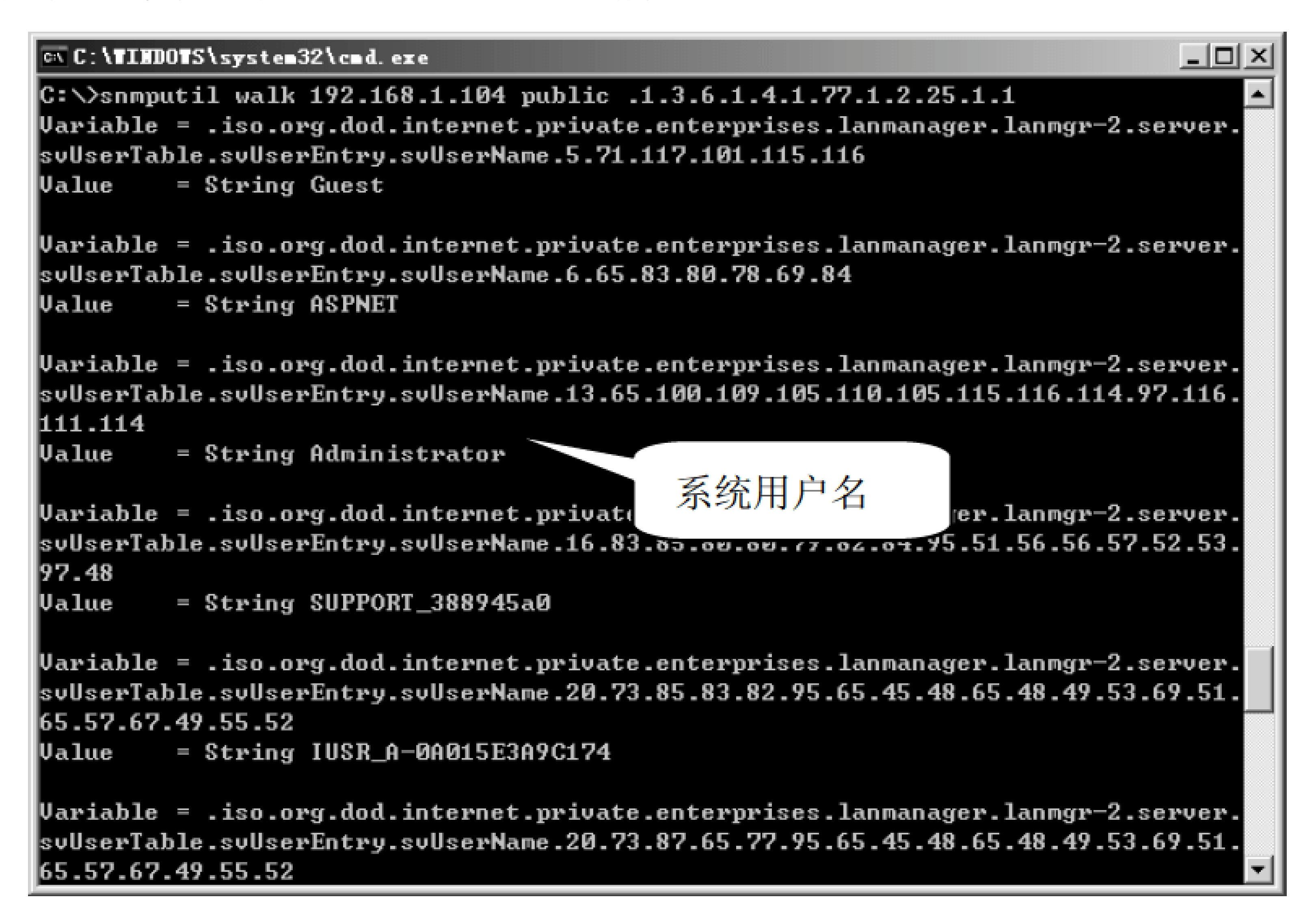


图 2-30

03 输入命令“snmputil walk 192.168.1.104 public .1.3.6.1.4.1.77.1.4.1.0”，按【Enter】键确认，即可显示设备使用的域名，如图 2-31 所示。

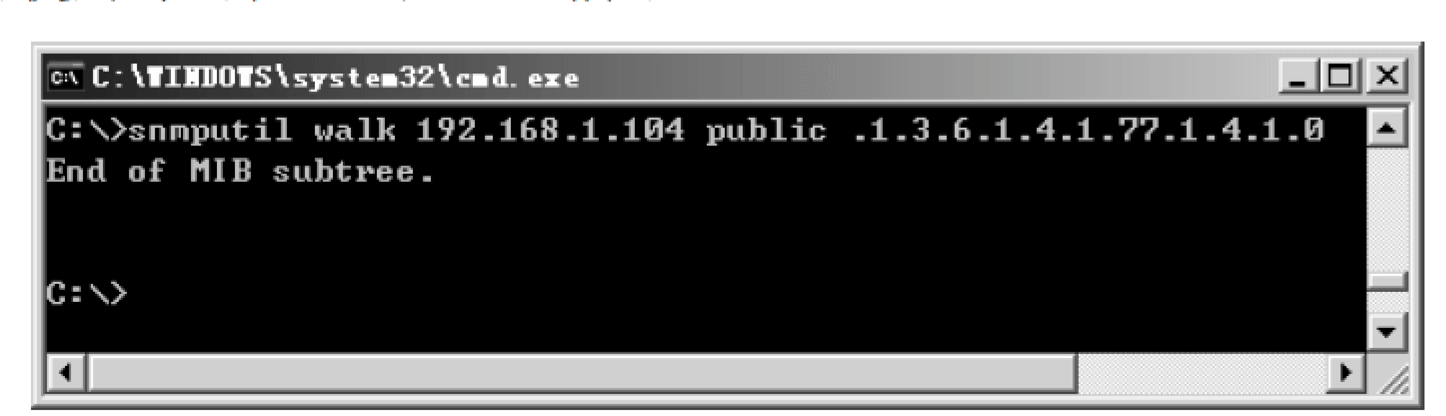


图 2-31



上述被管设备没有配置域名，所以没有结果显示。

04 输入命令“snmputil walk 192.168.1.104 public .1.3.6.1.2.1.25.6.3.1.2”，按【Enter】键确认，即可显示设备上安装的软件列表，如图 2-32 所示。



图 2-32

05 输入命令“snmputil walk 192.168.1.104 public .1.3.6.1.2.1.1”，按【Enter】键确认，即可显示设备的系统信息，如图 2-33 所示。

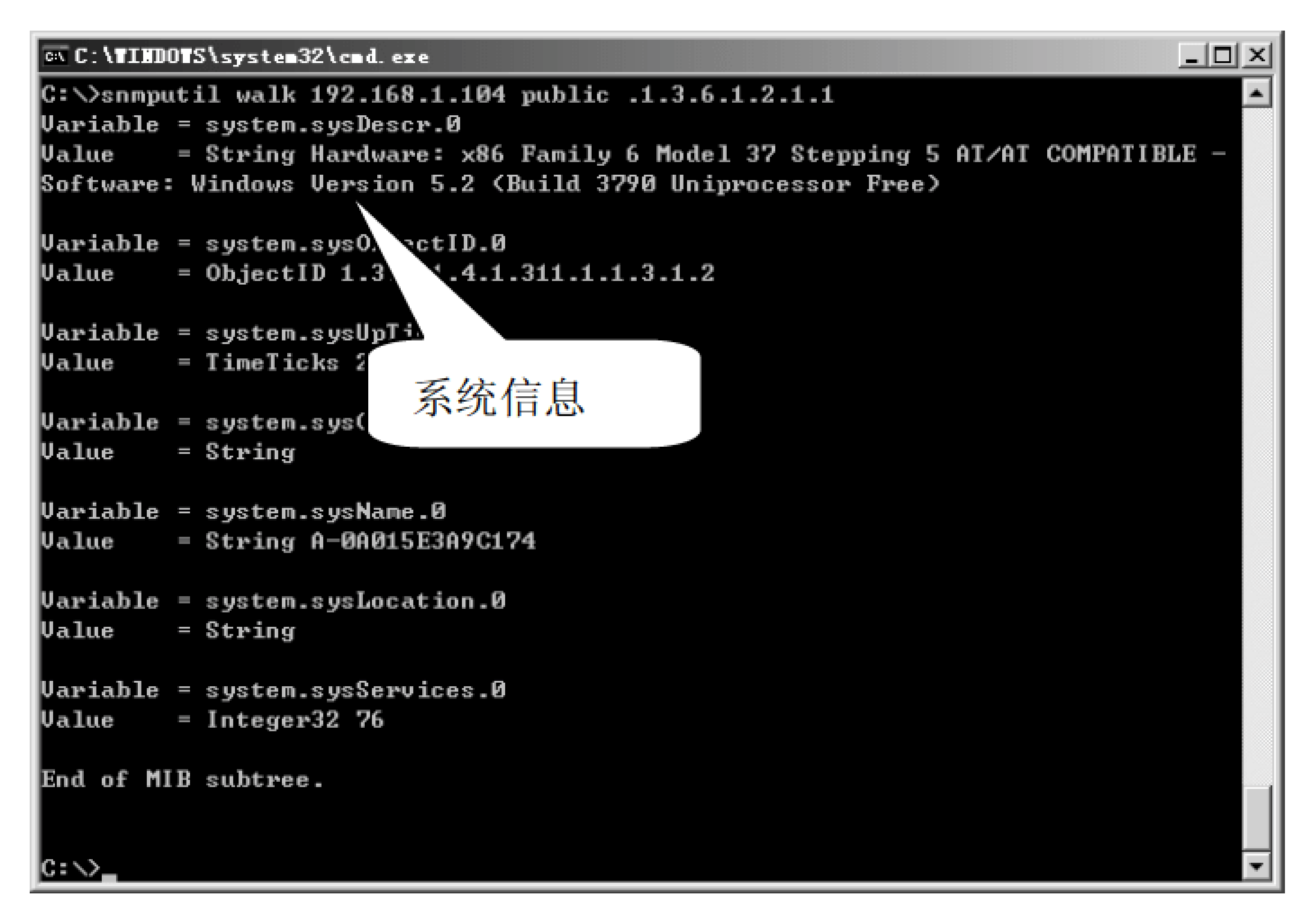


图 2-33

2.7　专家答疑

（1）SNMP 协议本身存在一些安全问题，应当如何确保 SNMP 管理安全呢？

答：目前 SNMP 主要有三个版本，其中 SNMPv1 和 v2 两个版本较弱，而 SNMPv3 采用了新的 SNMP 扩展框架，安全性和管理上有很大的提高，所以要尽量让网络环境支持 SNMPv3 的使用。

很多支持 SNMP 服务的产品的出厂设置中，默认的 community-string 值是“public”（只读访问）和“private”（读/写访问）。攻击者往往会使用这两个 community-string 扫描网络，实现网络攻击。

所以在配置设备时，这两个默认口令一定要改掉。

攻击者通常处于外部网络，通过向边界设备发送 SNMP 请求信息，以查找漏洞实现攻击。而 SNMP 协议只在内部网络正常运行即可满足管理的需要。所以，可以在边界设备外侧端口过滤所有的 SNMP 信息，以避免信息外泄和网络攻击。

在很多网络系统中实施网络管理时，只有个别的网络管理系统需要发生 SNMP 请求。所以，网络管理系统中的 SNMP 代理（被管客户机）可以设置仅接受管理服务器发送的 SNMP 请求。这样可以降低内部攻击风险。

（2）MIB 管理信息库结构层次复杂，除基本信息库外各个厂商还有 MIB 管理信息库，如果直接使用对象标识符的话很难记忆，在实际网络管理中应当如何使用呢？

答：由于网络管理信息量的庞大，导致 MIB 管理信息库很复杂。如果单靠 MIB 管理信息库对象的标识符去查看对应管理信息，根本就不现实。

一般各种网络管理产品生产时，都会自带有一定的 MIB 查询工具，使用这些工具不需要记忆对象标识符，可以利用工具直观的看到想要的信息。而且大部分网络管理软件都有自动扫描通用信息的功能，会以图标的形式显示出来，很少需要用户直接操作 MIB 信息库。

第 3 章　中小型企业网络管理项目概述与分析

网络技术发展至今，企业和社会的基础网络环境已经基本完善。而且近年来网络管理技术的越来越被重视，很多企业开始着手加强网络管理。对于一个现实的网络环境，如何实施网络管理呢？下面结合一个网络管理案例进行需求分析、方案设计及项目实施的讲解。

3.1　项目介绍

在进行网络管理分析之前，首先要了解企业概况、网络现状等信息。下面是案例企业的简介及网络概况。

1. 公司简介

某 IT 企业成立于 2004 年，主要从事软件开发及电子产品生产。在这七年时间里，企业有了飞速的发展，除了北京总部外，在全国各地还有多家子公司。北京总部员工数量比较多，有 200~300 多名，被分配在四个工作区。除此之外还有一部分员工需要经常出差移动办公。各个子公司员工数量相对较少，主要进行产品加工及分销工作。

2. 网络现状

网络现状可以总结为以下几点。

（1）全部使用 cisco 产品，并使用了三层交换机。

（2）总公司与子公司业务量比较少，采用 VPN 连接。

（3）对于移动办公用户和家庭办公用户使用远程访问 VPN 的方式访问企业服务器。

（4）在总公司内配置了供员工访问的 FTP、WEB、数据库等服务器。

（5）为了宣传企业形象，在公共网络 IDC 机房托管一台服务器，用于发布企业官方网站、OA 及邮件系统。

（6）企业总部用户使用全交换网络互联，为了减少广播使用了 VLAN 隔离。

（7）企业总部出口采用 10M 光纤，子公司一般采用 4M 宽带。

3. 网络拓扑

根据网络环境绘制如图 3-1 所示的网络拓扑图。

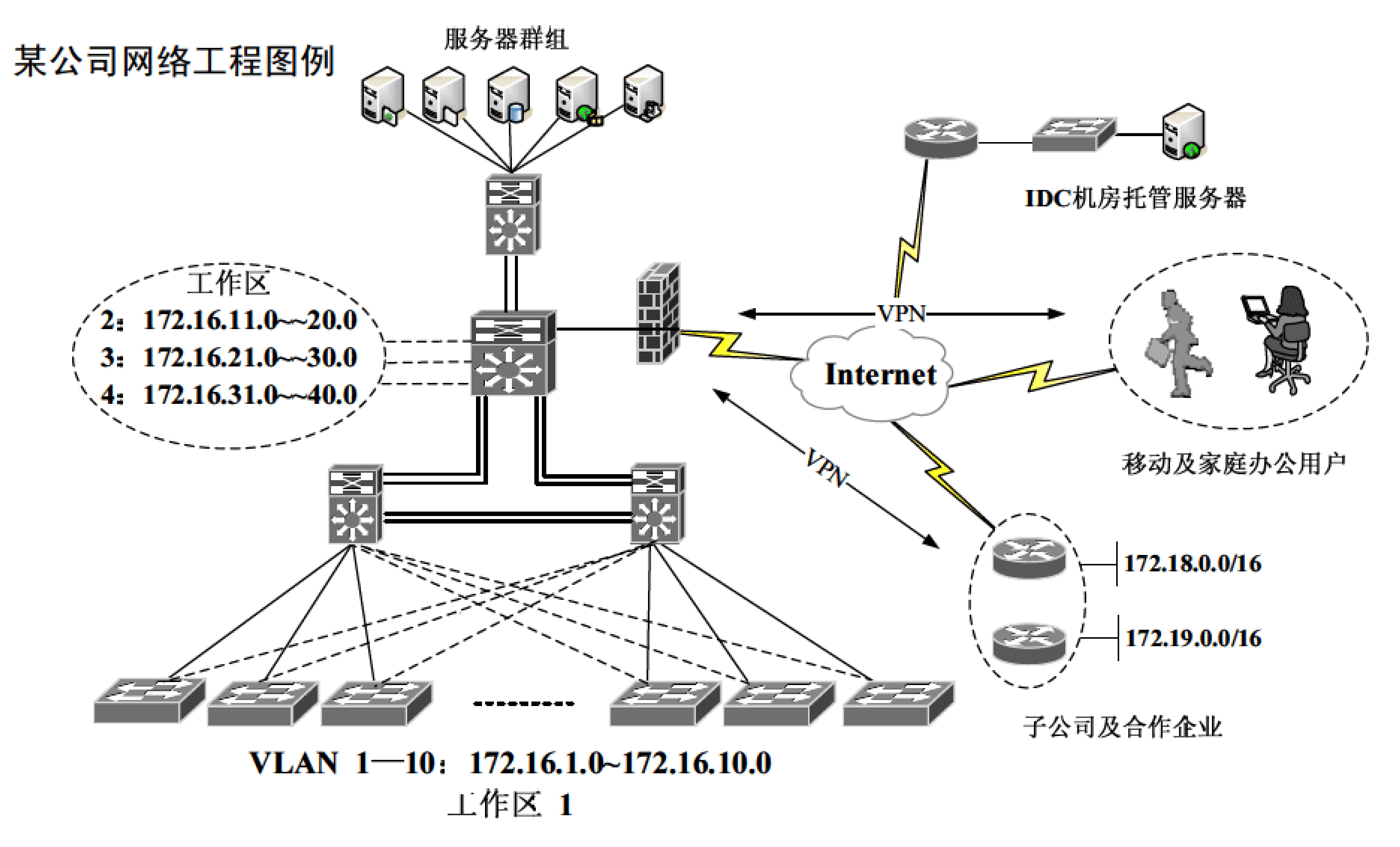


图 3-1

4. 网络管理现状

企业网络环境已成规模，但是网络管理依然落后，目前存在的网络管理问题有以下几点。

（1）网络内经常出现地址冲突现象，广播流量过大。

（2）虽然出口带宽为 10M 光纤，但是内网员工访问公网时网速依然不容乐观。

（3）企业网络故障恢复时效低，经常会因为网络故障影响公司业务及员工办公。

随着业务的扩展，企业对网络环境的可靠性、稳定性要求越来越高，必须完善现有网络的网络管理体系。

3.2 需求分析

结合网络管理现状，做出如下分析。

1. 网络内经常出现地址冲突

造成企业内频繁出现地址冲突的原因有两点。其一，现在使用移动办公设备的员工越来越多，新增的移动设备在没有充足 IP 地址的情况下，会被设置成其他固定台式机的 IP 地址，台式机地址被占用后为了能联网会更改其 IP，可能又和其他主机地址冲突，这样循环下去地址冲突现象会越来越严重。其二，木马病毒一直是电脑使用者头痛的程序，其中像 ARP 病毒就可以造成局域网地址冲突，如果一台电脑感染后，此病毒会迅速向网络中的其他主机发送地址欺骗信息，造成这些主机出现地址冲突现象，而且这类病毒极易传染。

解决办法：要解决地址冲突可以从两方面考虑，首先是地址不足，管理员在进行地址分配时可以多做冗余，比如 50 人的部门可以分配拥有 126 个可用 IP 的子网，同时再配置 DHCP 动态地址分配服务器，所有新增主机全部采用动态 IP 地址。其次所有关键设备，如路由器、交换机全部

配置 IP+MAC+端口的地址绑定，所有主机也可以执行地址绑定的脚本文件。

2. 广播流量过大

广播流量过大主要有两个原因，其一是广播域太大，其二是由病毒或木马引起的。本方案中已经做了较细致的 VLAN 划分，广播域已经被缩小，可以不考虑广播域的问题。病毒和木马都具有较强的传染性，当企业内的某台主机感染病毒或木马后，可能会向局域网内的其他主机发送大量广播信息，以实现网络攻击与传染。

解决办法：通过网络性能检测工具实时检测广播源，并及时隔离清除威胁。

3. 网速不容乐观

目前网络带宽已经有 10M 光纤，这对于一般企业来说已经够用了，所以造成网速较慢的原因可以从三个方面考虑。其一，局域网带宽被大量广播消耗掉了，很多网络都还是 100M 网络环境，如果短时间内出现了大量的广播流量，就会出现网络拥塞，导致网络访问请求延迟过高。其二，有个别用户在使用下载工具或观看在线视频，10M 光纤网络，带宽资源已经算是充足，但是依然有个限度的，如果网络内出现大量的视频或文件下载流量，必然会导致其他用户服务抢出口带宽。其三，网络攻击阻碍互联网访问，比如拒绝服务式网络工具，可以拥塞公网出口，使内网请求信息无法正常转发。

解决办法：可以在网络内架设流量监控系统，实施监控所有网络流量，通过监控系统可以分析出占用带宽的数据源，然后再使用网络管理工具断开这些主机的网络或限制其流量。同时还可以在网络设备上做访问控制，特别要限制视频流量和特殊网站流量通过出口设备。

4. 网络故障频繁

企业网络环境相对复杂，从企业建成发展至今，网络设备随着业务扩充不断的增加，新旧设备混合，再加上管理混乱，所以网络故障才会频繁发生。网络环境的负载如果不能满足通信的要求，过多业务流量会让网络处于超负荷工作状态，比如网络设备的背板带宽、传输速率、CPU 性能等。如果能在网络隐患刚刚出现，还处于萌芽状态时就将其扼杀，网络故障自然就少了。

解决办法：要经常进行网络性能分析，处于关键位置的设备需要有专门的程序实时地监控其运行状态、性能指数，在超出网络负载之前要做好升级改造工作。

5. 故障恢复时效低

故障恢复时效低和不健全的网络管理有直接关系，企业飞速的发展忽略了网络管理的重要性，一直采用传统的管理方式，即便是加入了一些网络管理设备，也因网络管理水平的限制而成为摆设。传统的网络管理几乎采用人工式的反应，故障发生之前很难察觉，当故障发生后才会被发现，而这时故障已经发生，已经造成了一定的损失，恢复起来相对难度会大一些，单是排查故障原因就需要耗费很多时间。

解决办法：建立网络管理平台，实时监控网络状态。通过网络管理平台准确找出故障点与原因，做针对性的故障恢复。

通过以上需求分析可以对网络实施相应的改造，具体网络改造内容可以总结为以下几点。

（1）建立网络基础信息档案，包括网络拓扑结构、设备数量、地址配置、功能实现、（MAC+IP+端口+用户）对应表等。以帮助管理员掌握网络，并为解决网络故障提供辅助资料。

（2）搭建网络管理平台，做到对整个网络的实时监控。

（3）对重点网络设备做性能的实时监测。

（4）对企业内网服务器和 IDC 机房托管服务器采用远程服务器监控程序，进行维护。

（5）架设网络流量监测分析程序，实时监控网络流量，以方便发现网络故障隐患及查找故障原因。

（6）运用安全的网络管理协议。

实施改造后企业网络拓扑结构没有太大改变，但是网络管理能力得到极大的提升，改造后的网络拓扑图，如图 3-2 所示。

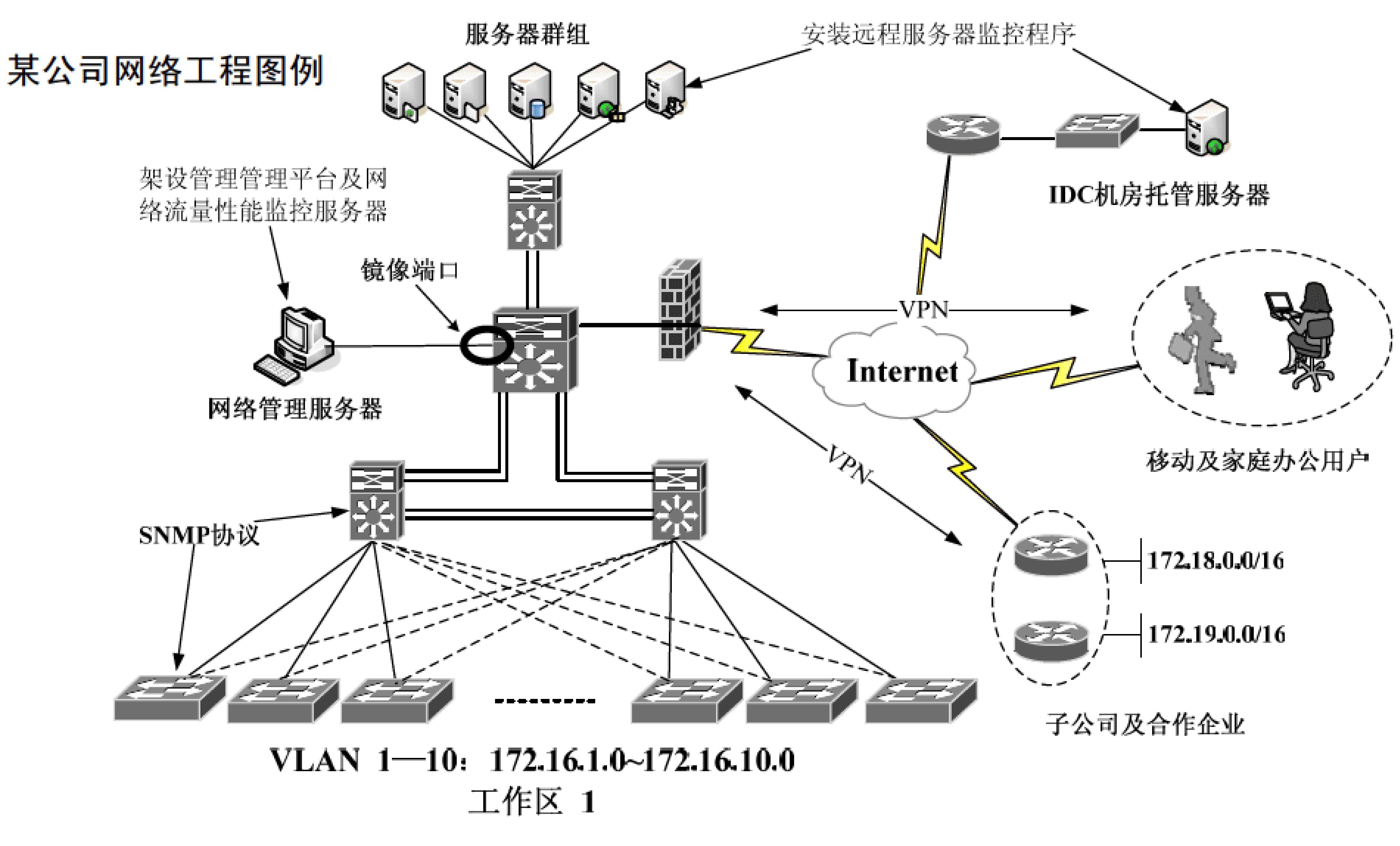


图 3-2

网络中加入了一台专门的网络管理服务器，用于安装网络管理平台和网络性能监控服务器等程序。在所有服务器安装了远程服务器管理程序的客户端。为了使网络管理服务器可以监控全网流量，在所有交换机中做镜像端口，流量镜像到网络管理服务器方向。在所有网络设备和计算机开启 SNMP 服务，配置安全的共同体，并配置必要的 trap 自陷消息。

3.3 项目实施流程

项目要采用分步实施的方式完成，结合上文的需求分析，网络管理方案可以做以下六步操作。

3.3.1 获取网络基本信息

获取网络基本信息是管理整个网络的根本，作为网络管理员，想要高效的完成网络管理任务，

首先要了解当前的网络结构，获取基本网络信息，比如网络规模、主机分布、IP/MAC/主机名/用户对应关系、设备数量及分布、设备型号及配置、主机及服务器（硬件）配置等信息。如果网络出现问题，就可以根据事先掌握的基本信息快速的找到故障点，并加以解决。

获取网络基本信息可以通过现场调查和网络扫描工具两种方式来实现。获取网络基本信息难度并不大，但是工作量确不小，使用网络扫描工具可以快速的获得需要的 IP、MAC、计算机名等对应信息，但还是有一些东西是无法用工具扫描到的，比如部门人员分配，这些无法扫描到的信息需要通过现场调查走访的方式获取。常用的网络扫描工具有 IPMaster（IP 地址管理工具）、MAC 地址扫描器等。

获取到网络基本信息后，可以建立网络基本信息库，此信息库可以使用表的方式体现。表 3-1 和表 3-2 为给出的参考样表。

表 3-1　员工网络地址统计表

姓名	部门	办公室	计算机名	IP 地址	MAC 地址	机器配置	联系电话	其他

表 3-2　网络设备信息统计表

网络设备	地理位置	设备名	硬件配置	功能作用	地址配置



网络基本信息统计表要根据企业环境需求进行设计，一定要做到准确、结构清晰、易查找。

3.3.2　搭建网络管理平台

企业内的网络设备比较多，链路连接也比较复杂，一旦发生网络故障，管理员很难在第一时间找出故障原因，需要经过长期的排查。而在企业里，每一分钟的业务中断都有可能造成巨额的损失，必须要尽量的缩短故障恢复的时间。想要缩短故障恢复时间，需要有良好的故障恢复能力，同

时也需要有更好的方法查找网络故障原因。

网络管理平台，又叫网络运维系统。通过该系统可以实时地获取网络拓扑信息，网络设备的配置、性能信息，如果设备出现异常会通过各种图表进行显示，同时还可以根据阈值进行报警提示。这样一来网络性能指标超过阈值时管理员就可以知道，通过调试可以避免严重的网络故障发生，如果网络故障真的发生了，也可以通过网络管理平台清晰的找到故障点及故障原因。

搭建网络管理平台需要在网络管理服务器上安装管理平台软件，并在所有被监控的设备上运行 SNMP 协议。搭建网络管理平台可以按照图 3-3 实施。

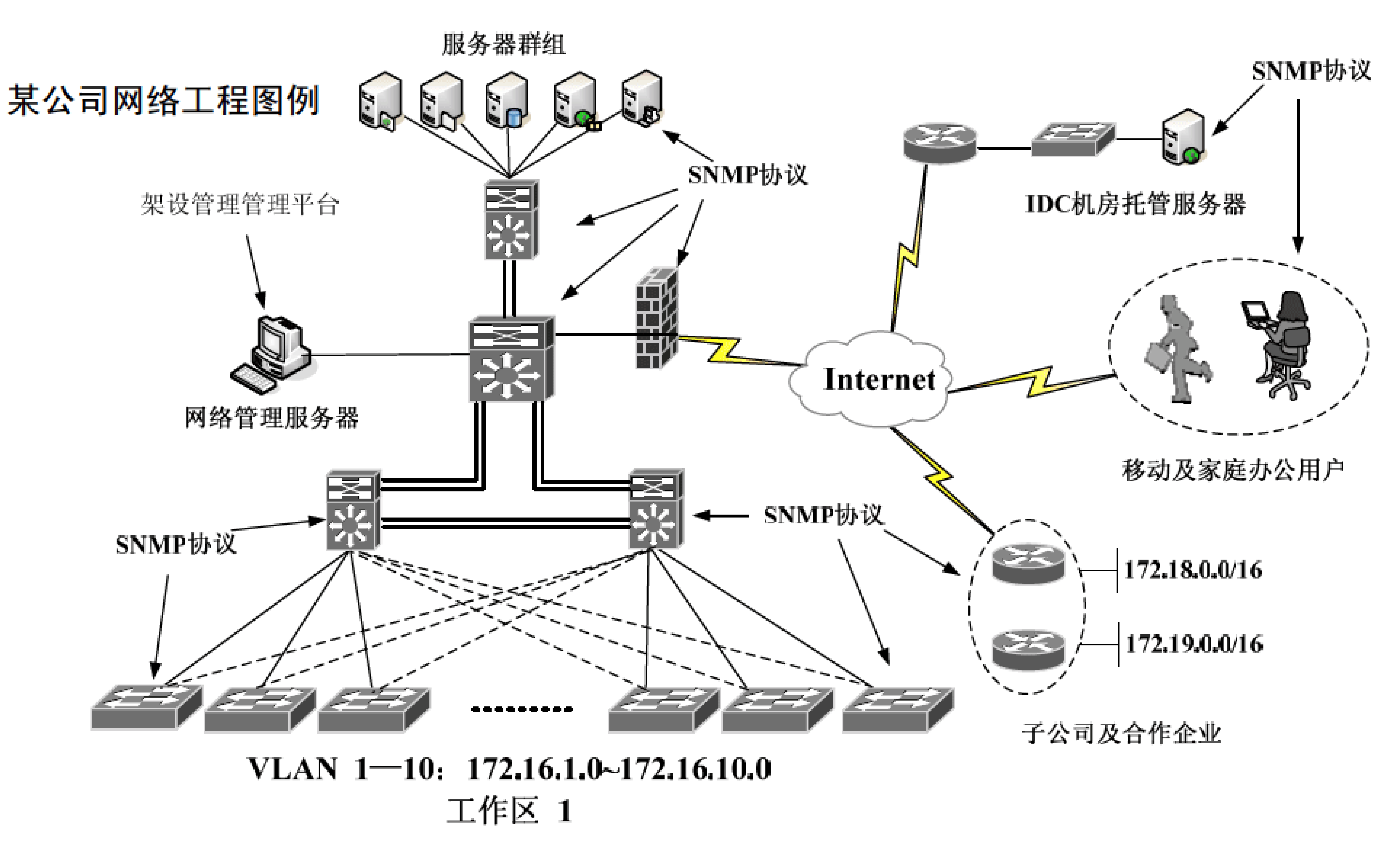


图 3-3

目前使用的比较多的网络管理平台有 Spiceworks、WhatsUp Gold、HP OpenView、IBM Tivoli NetView，除此之外还有很多类似软件，但是大部分软件在使用上都大同小异。

3.3.3 监控重点网络设备

企业网络里的个别设备处于关键位置，一旦损坏将对整个网络的运作造成巨大的影响，所以要采用专门的工具监测这些设备的运行状态，一般监测的有 CPU、出入流量统计等信息。

很多工具里面都包含有这项功能，比如网络管理平台和网络流量性能监控系统。除了以上程序自带该项功能外，还可以使用 SolarWinds 工具，该工具是一套非常全面的网络管理工具，可以实现中多网络管理需求，其中值得注意的是该工具专门嵌入了 Cisco 设备管理功能。对网络设备进行监控时不需要过多操作，只要确保设备开启 SNMP 协议即可。

根据设计可以做出如图 3-4 所示的调整。

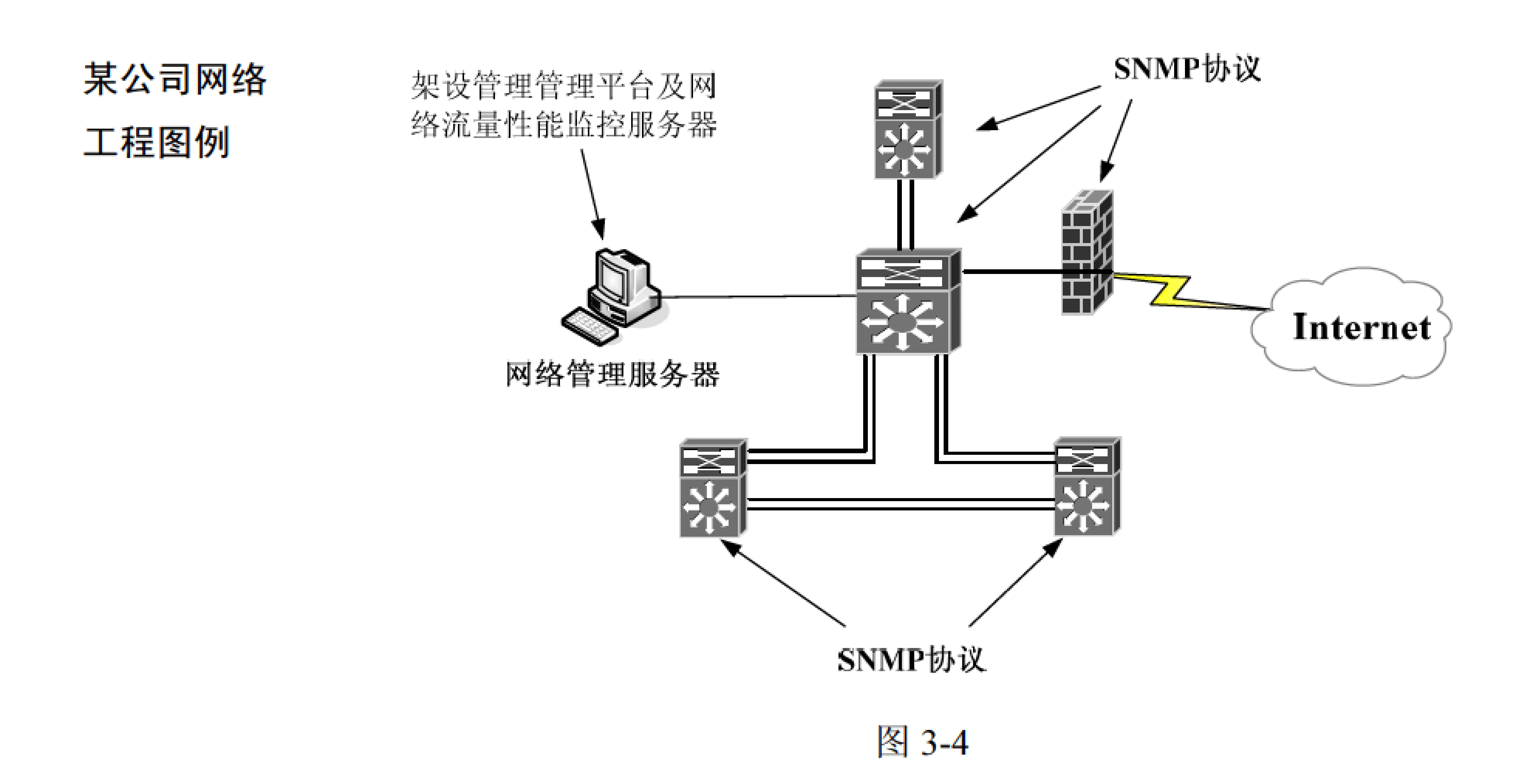


图 3-4

3.3.4　实现服务器远程控制

企业的大部分工作都需要内外网服务器作支持，所以企业内网络服务器和 IDC 机房托管服务器稳定性至关重要，必须要实时监控这些服务器的性能，并且要有安全可靠的远程管理手段完成服务器的监控与配置。

传统的方式是采用 Windows 自带的远程桌面连接功能，这样做虽然可以直观地操作远程服务器，但是安全性较弱，任何主机只要知道地址和账户都可以连接，并且这样只能做到对远程服务器的控制，却不能实时获取远程服务器的性能信息，需要另找程序监测性能。

除了传统方式外，还可以采用 SSH、VNC 和其他专业远程服务器管理工具，这些方法一般都带有较为严格的认证加密手段，部分方法除了指定的管理服务器外，其他主机很难对服务器进行管理控制。可按照图 3-5 实施服务器远程控制。

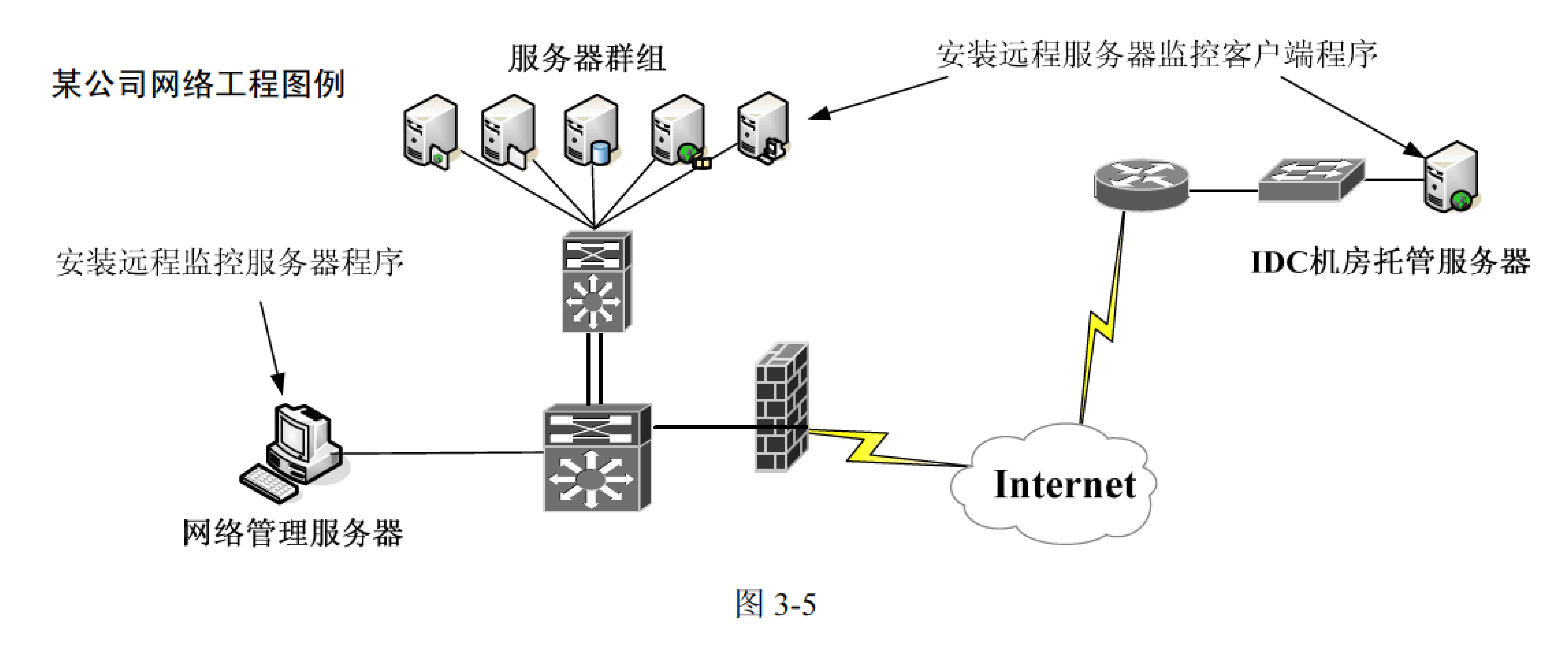


图 3-5


提　示

对于 IDC 机房的托管服务器，在实施远程管理时可能会产生特殊的管理数据流，这些流量需要被出口的防火墙设备转发，应注意防火墙的访问控制策略。

3.3.5 加强员工网络安全管理意识

在企业网络中，管理员做的最多的工作是为普通用户做机器维护。由于普通员工的计算机使用水平不一样，很多用户不能合理的使用计算机，一旦遇到计算机故障就不知该如何处理。所以作为管理员，一定要具有较高的单机故障维护能力，多准备一些故障维护盘。

造成网络中单机维护工作过多的原因除了员工操作水平不高外，和单机的安全防护能力弱也有直接关系。很多员工在使用计算机时不注意个人主机的安全，没杀毒软件，没漏洞检测软件，“裸机”上阵的很多，这些机器极易感染病毒木马，一旦被网络攻击者利用，很有可能成为威胁整个网络的隐患。所以在实施网络管理改造中，可以适当的对员工进行计算机基础应用培训，让员工安全的使用计算机，并掌握独立解决小故障的能力。

3.3.6 故障检测与分析

在网络管理中，经常出现网速慢、地址冲突频繁、出现大范围网络攻击等现象，这些故障一般都不是硬件造成的，想要找到故障原因，难度很大，目前最有效的方法就是通过分析网络数据流查找异常信息流。

当机器感染了 ARP 病毒后，会迅速向全网发送地址欺骗信息，通过网络流量监测分析工具可以清晰地看出是哪台主机在发送大量的 ARP 信息，结合之前统计的网络基本信息可以很快找到感染病毒的主机用户，让其进行病毒的查杀。

如果网速变的很慢，也可以通过流量监测分析工具对全网进行流量分析，找出比较占用带宽的数据流。通过查看单位时间内哪台主机接收数据包最多，就可以判断出带宽严重浪费的原因。

每种网络故障都有独特的网络异常流量，这里不再做过多的介绍。这里有另外一个问题需要考虑，网络环境中的流量这么多，想要实现流量监测就必须让所有流量通过网络流量性能监控服务器，广播流量还好说，但是如何确保跨网段流量和单播流量都流经流量性能监控服务器呢？这需要在所有网络设备上做一项技术配置：镜像端口。通过镜像端口技术，可以把交换机多个端口的流量分别做一份数据镜像转发到镜像端口，所有的镜像端口都向着网络流量性能监控服务器方向配置，就可以实现全网流量监控。

根据设计可以做出如图 3-6 所示的调整。

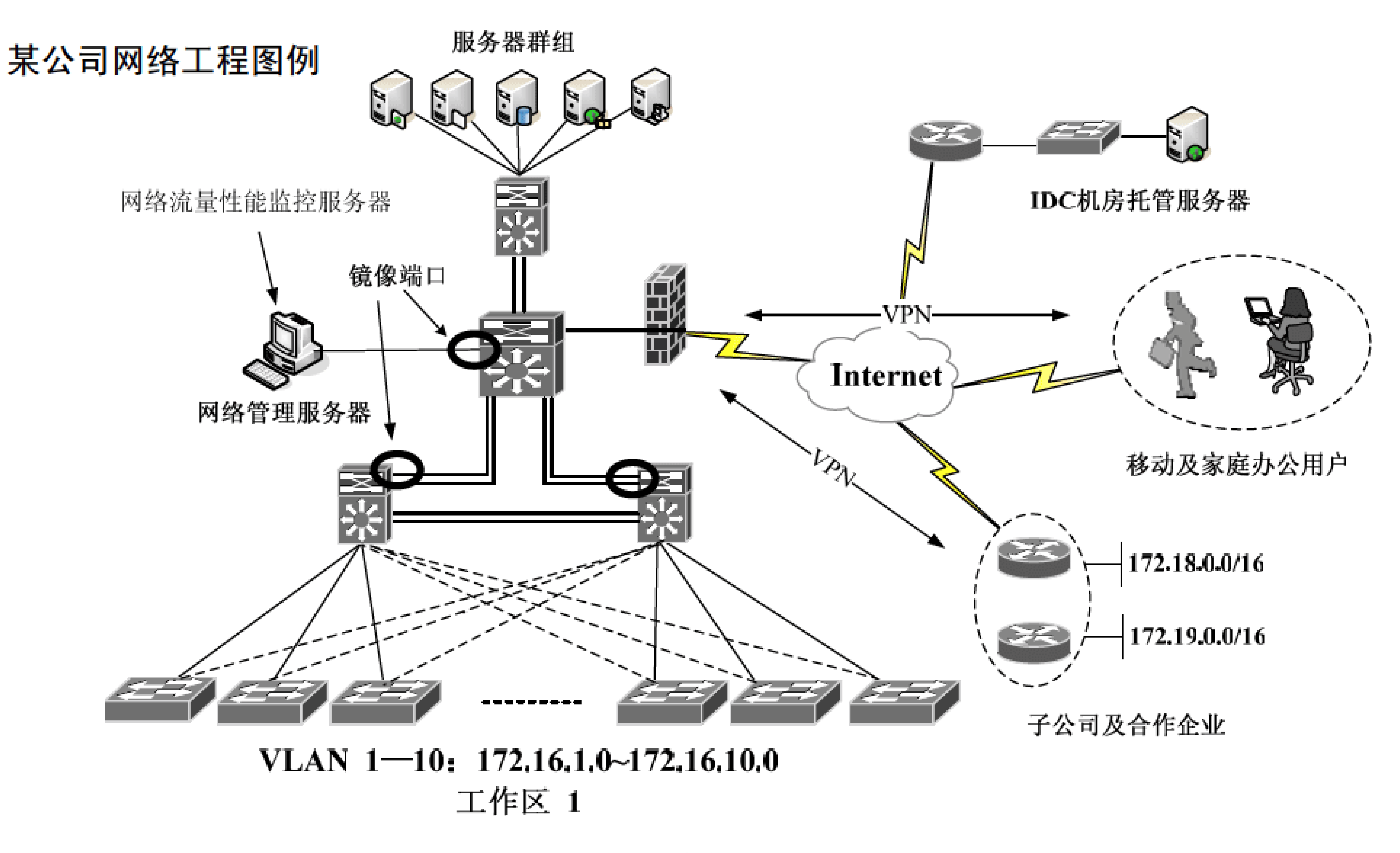


图 3-6

3.4　专家答疑

（1）按照本章节网络管理方案实施，是否可以达到较高的网络管理质量？

答：各种网络管理工具的实施都不是促成高效网络管理体系的重点，工具只是网络管理体系中的辅助工具，关键还是要依靠网络管理员自身的素质。

如果拥有高端的网络管理工具，而网络管理员却不懂得如何使用，不主动的进行网络性能分析，故障扫描，不能及时有效的解决网络故障，那所有的网络管理投入就没有意义了。

网络管理是很细致、很繁琐的工作，需要网络管理员实时的关注网络状态、网络性能，时刻为网络运行状况着想。有了管理员认真、踏实的工作，加上高效的网络管理工具，才能达到网络管理质量的最大化。

（2）网络信息这么多，如何从这些信息中找到有用的管理信息？

答：网络管理信息的收集要和网络管理的最终目标相结合，网络管理的目的就是为了掌握网络环境状况，获知网络性能，找出网络故障隐患，使网络更稳定、更高效的运作。

除了获取网络系统配置信息外，网络性能信息也很重要，可以依靠专门网络管理工具获得。但是很多网络隐患是不能直接从性能和系统配置上看到的，比如 ARP 攻击，广播风暴。这些需要网络管理员利用专业的流量监测分析工具进行操作。

流量监测分析工具可以抓获网络中的所有信息，但是真正能够构成网络威胁的可能只有不到一成，如何在大量的网络信息流中找出有用的流量呢？这就需要管理员了解所有网络流量异常的特征，比如如果发现网络中每秒中的广播流量都有几百以上，那就很有可能发生了广播风暴，又比如在流量中发现了大量数据包，大小一样且小于 64 字节，可能是遭到了拒绝服务式攻击。网络管理信息很多，作为网络管理员，一定要有耐心。

第 4 章　获取网络基本信息

伴随计算机网络的普及和计算机应用技术的发展，企业网络设备的数量与种类越来越多，网络结构也变得越来越复杂。作为网络管理员，想要高效的完成网络管理任务，首先要了解当前的网络结构，获取基本网络信息，比如网络规模、主机分布、IP/MAC/主机名/用户对应关系、设备数量及分布、设备型号及配置、主机及服务器（硬件）配置等信息。如果网络出现问题，就可以根据事先掌握的信息快速的找到故障点，并加以解决。

4.1　网络基本信息概述

随着企业信息化的发展，网络的规模越来越大，网络中的主机数量越来越多，网络维护越来越难，网络故障解决的时间越来越长，已经影响到了企业的办公效率。做为网络管理员，首先需要做的就是掌握整个企业网络的规模和设备分布，其次是网络中的服务器信息和主机信息，包括计算机的 IP 地址、MAC 地址、用户，计算机硬件配置等信息，这些信息可以帮助网络管理员快速定位到主机或者设备的物理位置，从而加快解决故障的速度。因此，经常把网络拓扑图、网络中设备或者主机的分布图、主机的 IP/MAC/用户对应关系，设备硬件配置等信息称之为网络基本信息。

网络拓扑图和网络设备分布图可以通过实地调查获得，但是对于网络中主机的 IP/MAC/用户对应关系就不是那么容易能够获取到的，特别是网络中存在 DHCP 服务器时，客户端每次获取的 IP 地址是不同的，要准确地获取每个计算机或者设备节点的基本信息更是难上加难，更别说快速的找到某台计算机了，这时候就需要事先制作 IP/MAC/用户映射关系表，当网络出现问题的时候，可以通过数据包分析，通过 IP/MAC/用户映射关系表找到具体故障主机或者设备的物理位置。

MAC 地址又叫硬件地址，在 OSI 七层模型中位于第二层数据链路层，用来定义网络设备的物理位置。MAC 地址是烧入在设备芯片上的一个 48 位二进制数字，由 IEEE 协会统一分配，在网卡出厂的时候具有全球唯一性，在实际使用的过程中至少需要的在局域网中的唯一性，因此要定位网络中设备的唯一性，借助于 MAC 地址就很方便。但是 MAC 地址是 48 位二进制数，不容易记忆，这时候就产生了在网络层寻址的 IP 地址。

IP 地址又叫逻辑地址，在 OSI 七层模型中位于第三层网络层，用来进行网卡等网络设备的第三层寻址，是主机在互联网中的唯一标识。IP 地址是由 32 位二进制数字组成的，由国际组织 NIC 统一分配，计算机在使用互联网的过程中必须获取全球唯一的 IP 地址。在网络通信过程中，相邻节点间通信需要用到 MAC 地址，而不同网络间通信就要用到 IP 地址，因此 IP 地址和 MAC 地址

在计算机通信过程中起着非常重要的作用。但是不管是 IP 地址还是 MAC 地址，都是二进制数字，枯燥而不容易记忆，因此人们给每台计算机设置了通俗易记的计算机名称，当然计算机名称只在本地有意义。

局域网经常出现 ARP 攻击问题，当源主机在请求 ARP 解析的时候，ARP 病毒伪装目的主机的 MAC 地址返回给源主机，这时候源主机就会对接收到的错误目标 MAC 地址进行访问，使得网络内部出现大量的广播流量影响网络效率，对于这种问题的解决就需要用到网络基本信息。首先对网络数据包进行分析，查询哪些主机发送大量的 ARP 包，这些主机可能就感染了 ARP 病毒，通过这些数据包的源 MAC 找到该计算机的使用用户，从而解决问题。

4.2 获取网络基本信息

网络管理员在进行网络管理之前，首先应该想办法获取网络中所有设备的基本信息，避免在网络出现故障的时候，因为难以定位故障节点而影响网络的修复。常见的获取网络基本信息方法有两种：工具扫描和走访调查。

4.2.1 工具扫描

面对大量的客户端，工具扫描是个不错的方法。工具扫描是指在局域网中任意一台计算机上安装扫描工具，然后扫描局域网所有正在运行的计算机以获取网络基本信息。

如图 4-1 所示是用 MAC 地址扫描器扫描局域网中计算机基本信息的效果。



图 4-1

4.2.2 走访调查

面对大量的客户端，工具扫描可以统计出全部正在运行的计算机或者网络设备的网络基本信

息，但是每个计算机或者网络设备的物理位置等信息是无法统计到的，这些还必须依靠人工走访调查来进行统计，以完善网络基本信息。

4.3 IP/MAC 地址查看工具

可以使用的 IP/MAC 地址查看方法很多，下面介绍几种常用的命令及工具。

4.3.1 Windows 系统内置工具——ipconfig

ipconfig 是内置在 Windows 的 TCP/IP 应用程序，用于查看计算机本地网络适配器的计算机名称、IP 地址和 MAC 地址等 TCP/IP 信息，ipconfig 主要用于手工检查计算机的 IP 地址配置。另外在 DHCP 服务器存在的网络中，ipconfig 命令还可以用于释放和获取 IP 地址信息。

1. 查看本机的 IP 地址信息

使用 ipconfig 命令查看 IP 地址信息的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“cmd”命令，单击【确定】按钮，如图 4-2 所示。



图 4-2

02 弹出命令提示符窗口，在其中输入“ipconfig”命令，按【Enter】键确认，显示出“Windows IP Configuretion”信息，包括 IP Address（IP 地址）、Subnet Mask（子网掩码）和 Default Gateway（默认网关）等，如图 4-3 所示。

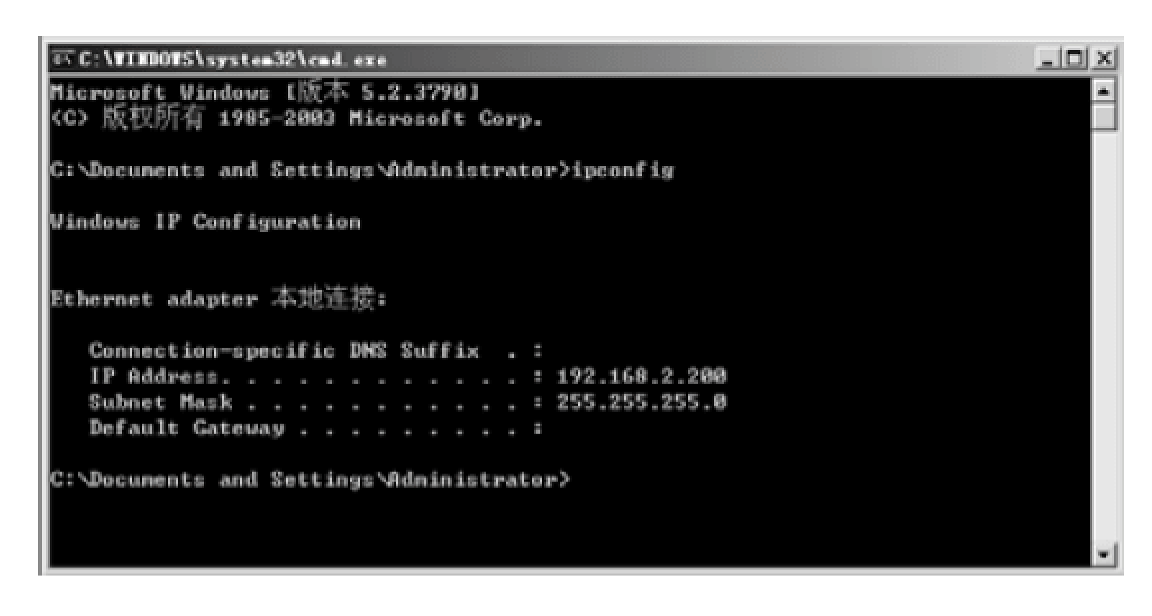


图 4-3

2. 查看本机的 MAC 地址

在命令提示符窗口中，输入“ipconfig /all”命令，按【Enter】键确认，显示出“Ethernet adapter

本地连接”信息，包括 Description（描述）、Physical Address（物理地址）、DHCP Enabled（DHCP 服务器是否开启）、IP Address（IP 地址）、Subnet Mask（子网掩码）、Default Gateway（默认网关）等，如图 4-4 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : howin-1f80af4ed
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : AMD PCNET Family PCI Ethernet Adapter
   Physical Address. . . . . . . . . : 00-0C-29-5A-3C-97
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 192.168.2.200
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>_
```

图 4-4

3. 释放本机的 IP 地址

在命令提示符窗口中，输入“ipconfig /release”命令，按【Enter】键确认，会看到本机的 IP 地址被释放掉，如图 4-5 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig /release

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 0.0.0.0
   Subnet Mask . . . . . . . . . . . : 0.0.0.0
   Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>_
```

图 4-5

4. 从 DHCP 服务器上重新获取 IP 地址

在命令提示符窗口中，输入“ipconfig /renew”命令，按【Enter】键确认。会看到本机重新获得新的 IP 地址，如图 4-6 所示。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

图 4-6

4.3.2 IP 地址管理工具——IPMaster

IP 地址管理工具是提供对 IP 地址使用以及 IP 地址划分的工具软件，它除了可以提供可视化的 IP 地址分配功能外，还可以对网络进行简单的管理，比如 Ping、TracertRoute、Telnet 等功能。使用 IP 地址管理工具可以大大提高网络管理人员的工作效率，该软件最主要是为了有序和高效的实现大中小型企业网 IP 地址的分配和管理。

IPMaster 是共享软件，用户可以通过各种渠道免费得到它的拷贝，也可以在不修改软件的前提下自由传播它。本软件为绿色软件，无需安装，直接运行可执行程序即可，试用版的有效期为 2 个月，因此在实验环境下可以选用试用版，如果要长期使用，可以进行购买注册。下面介绍使用 IPMaster 对 IP 地址进行管理的操作方法。

1. 新建管理网段

使用 IPMaster 工具，首先要制定管理网段，新建管理网段的具体操作步骤如下。

01 启动 IPMaster 软件，弹出【登陆】对话框，在【请输入登录密码】文本框输入 IPMaster 登陆密码，初次登录默认为空密码，单击【确定】按钮，如图 4-7 所示。

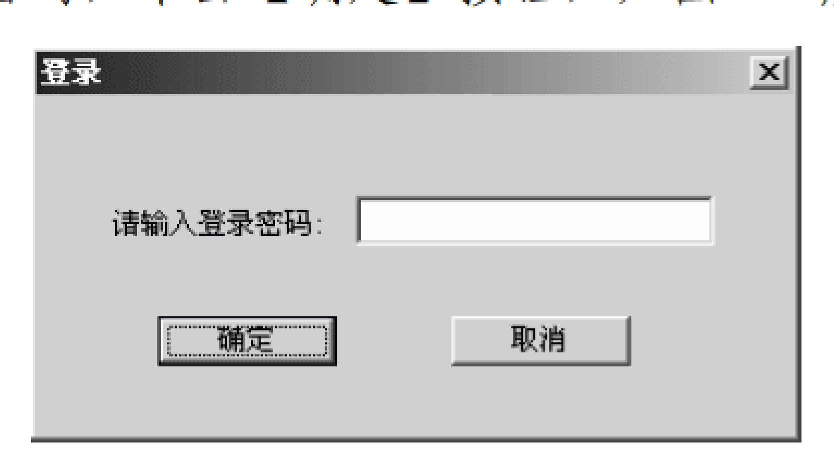


图 4-7

02 弹出 IPMaster 主界面窗口，选择【文件】➢【新建管理网段】菜单命令，如图 4-8 所示。

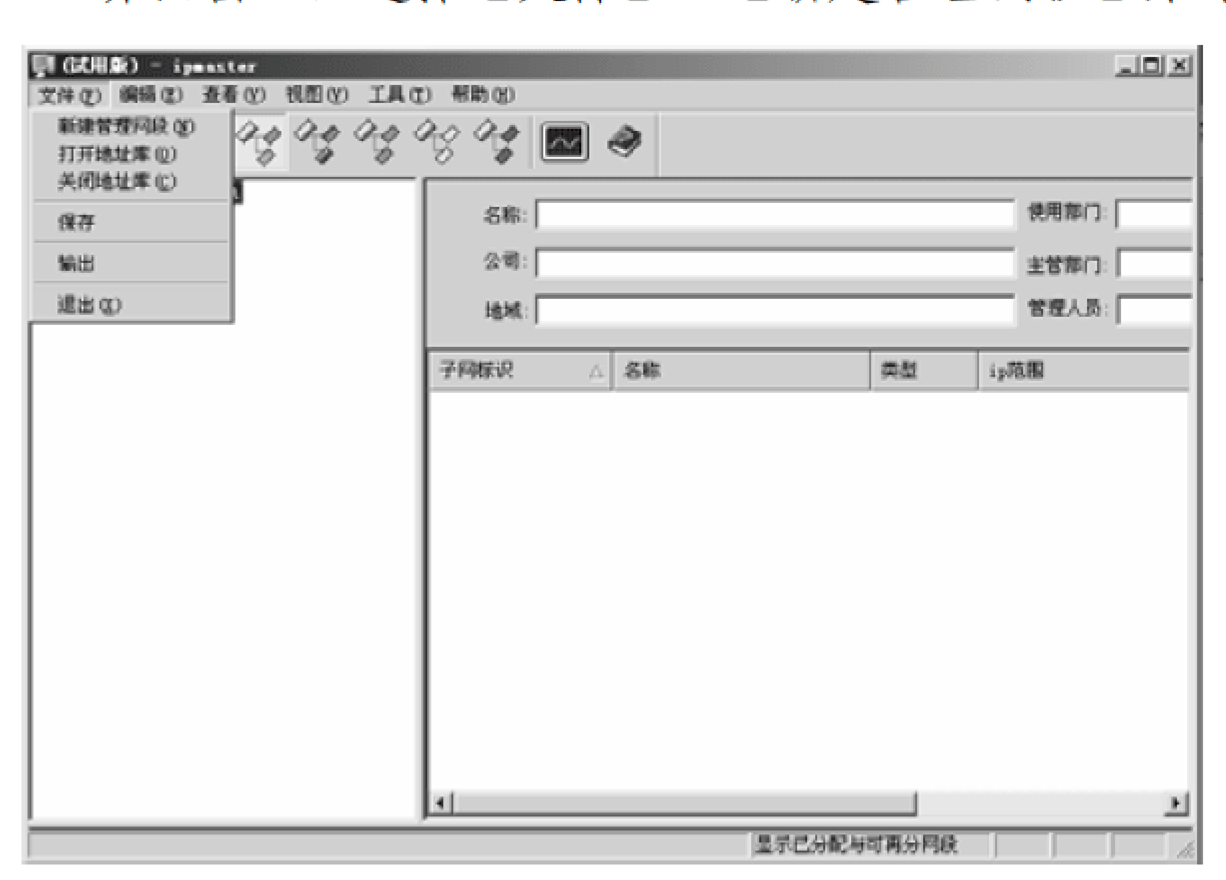


图 4-8

03 弹出【新建管理网段】对话框，在【网段名称】文本框中输入自定义的需要管理网段名称，在【网段地址】文本框输入要管理的网段，【网络掩码】文本框输入要管理网段的网络掩码，单击【确定】按钮，如图 4-9 所示。



图 4-9

04 系统会在树形拓扑图的【IPMaster-Root】节点下新建一个网段，就是需要管理的网段，如图 4-10 所示。

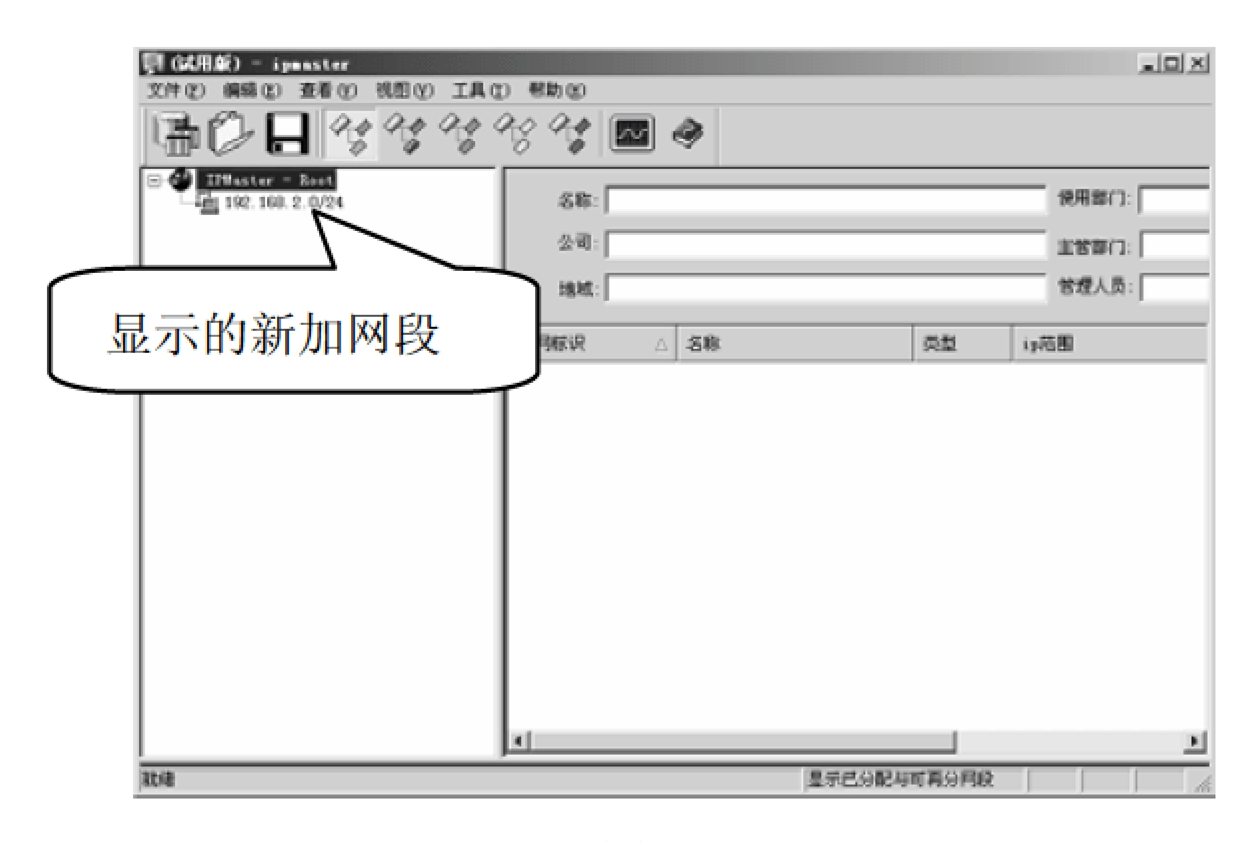


图 4-10

2. 子网划分

随着网络规模的扩大，网络中 IP 地址越来越紧张，同时大的网络也会带来广播的急剧增加。为了解决这些问题，可以根据网络中主机数量的多少，对 IP 地址进行子网划分。IPMaster 对子网划分有两种，手工划分和自动划分。子网划分的具体操作步骤如下。

01 右击建立好的管理网段，在弹出的快捷菜单中选择【划分】选项，如图 4-11 所示。



图 4-11

02 弹出【划分子网】对话框，通过该对话框可以选择子网划分的方式，选择【自动划分】单选按钮，单击【下一步】按钮，如图 4-12 所示。

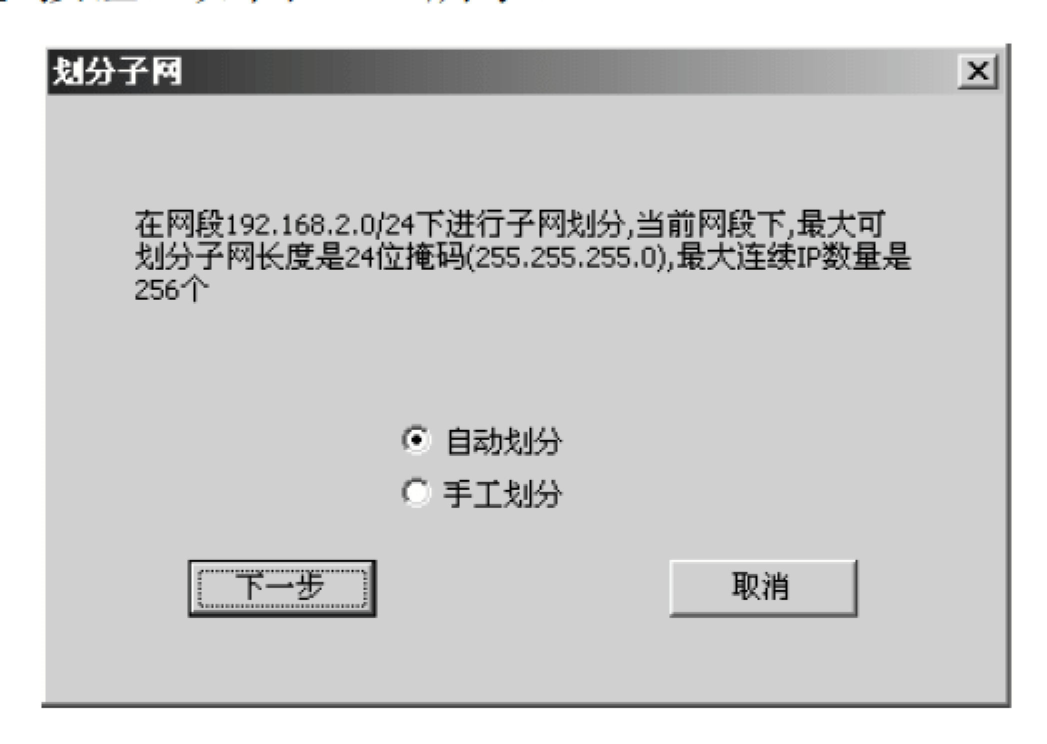


图 4-12

03 弹出【自动划分】对话框，在【划分的子网数量】和【子网中的主机数】文本框中分别输入要划分的子网数量和每个子网中的主机数，单击【下一步】按钮，如图 4-13 所示。

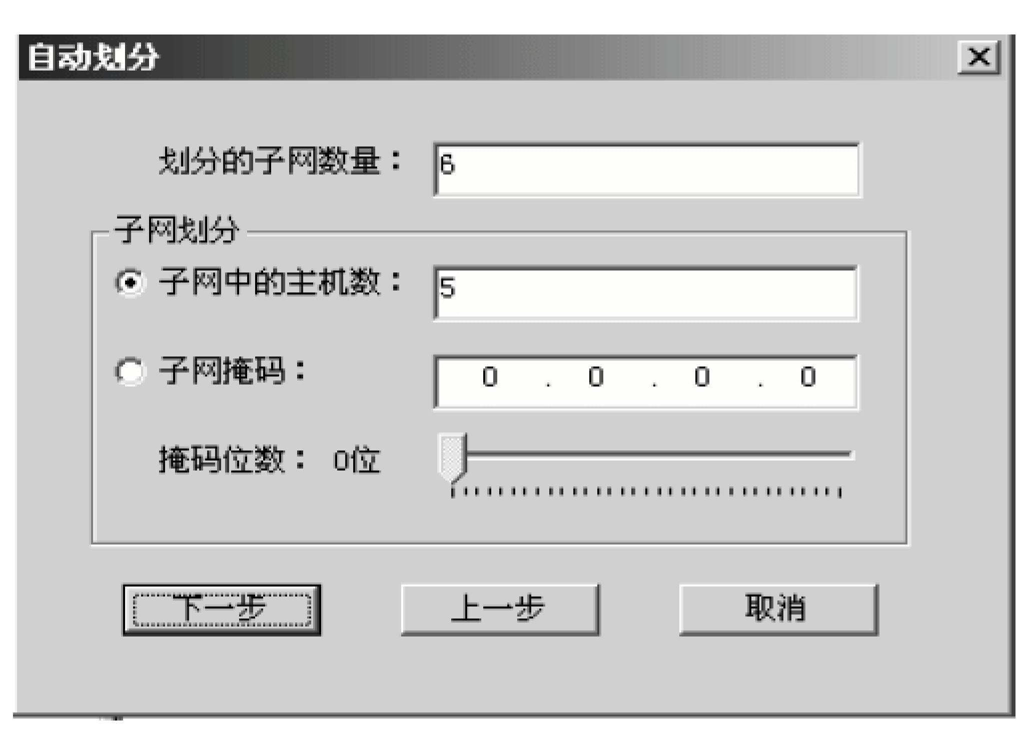


图 4-13

04 弹出【确认】对话框，核查划分的子网是否满足需求，单击【类型】下面的【已分配】下拉菜单，可以将子网状态修改为【已分配】、【可再分】和【保留】三种状态，单击【确定】按钮，如图 4-14 所示。



图 4-14

05 子网划分成功，返回【IPMaster】窗口，如果要对某个子网进行扫描管理，检查 IP 地址

使用情况，可以右击要扫描的网段，在弹出的快捷菜单中选择【扫描】命令，如图 4-15 所示。

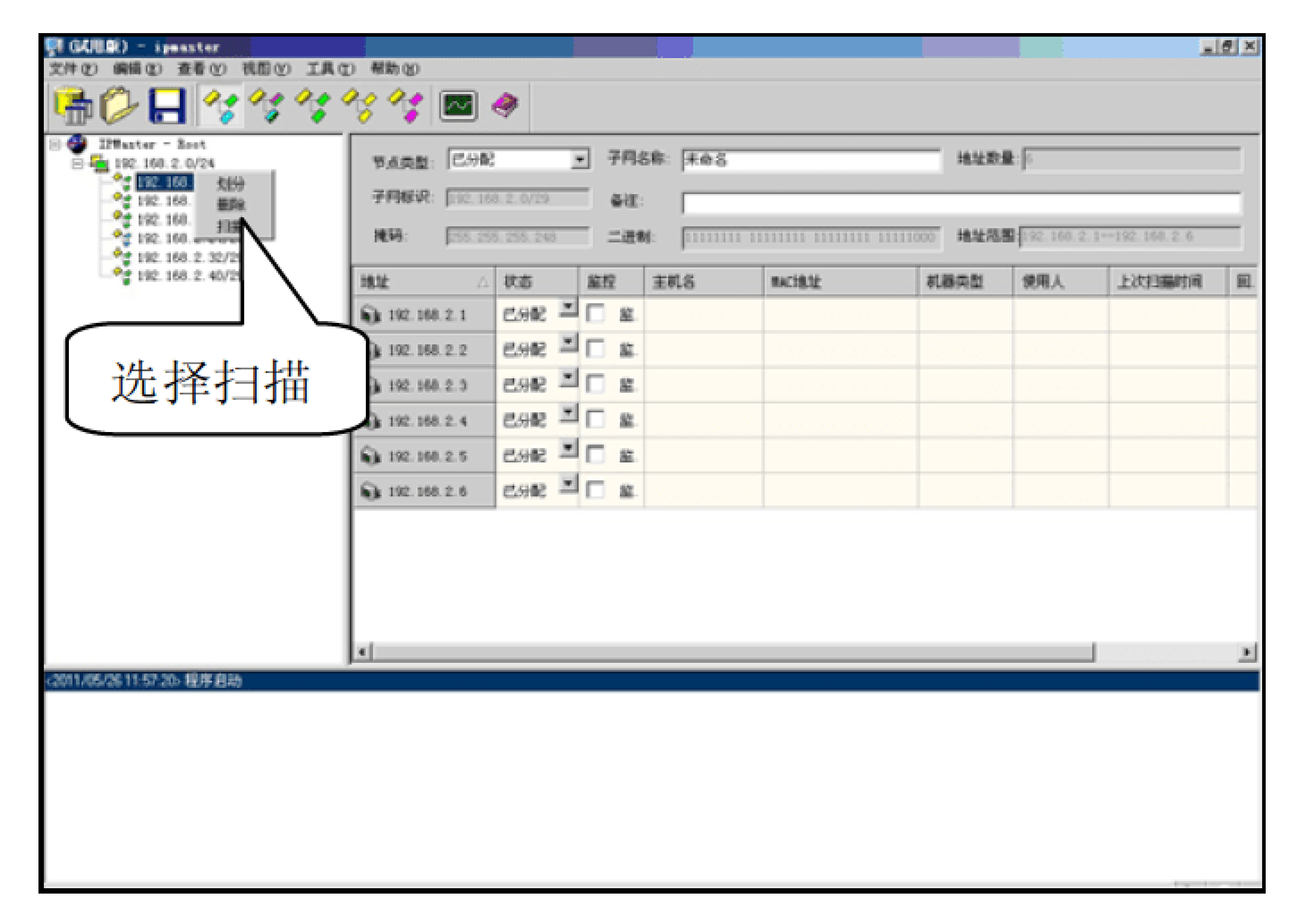


图 4-15

06 扫描成功，返回【IPMaster】窗口，看到该子网 IP 地址分配情况，包括网络中计算机的 IP 地址、主机名、MAC 地址等网络基本信息，如图 4-16 所示。



图 4-16

3. 监控与管理网络中客户端

IPMaster 除了管理网络中 IP 地址分配情况和扫描基本网络信息外，还可以测试客户端的网络连通性，具体的操作步骤如下。

01 选中想要监控的计算机的【监控】选项，如图 4-17 所示。



图 4-17

02 在菜单栏中选择【工具】➢【监控】菜单命令，弹出【监控】对话框，在【监控间隔】文本框中输入监控间隔时间，单击【确定】按钮，如图 4-18 所示。



图 4-18

4．网络连通性测试

当网络出现异常时，可以利用 IPMaster 软件的连通性测试工具，具体操作步骤如下。

01 右击要测试的主机 IP，弹出各种网路连通性测试命令，如图 4-19 所示。



图 4-19

可用的网络测试命令功能介绍如下。

（1）【ping】：测试网络连通性。

（2）【traceroute】：路由跟踪命令，测试源地址达到目的地址经过的路由节点。

（3）【telnet】：远程登录命令，后跟目的 IP 地址。

（4）【net send】：发送信息，需要对方开启 message 消息服务。

02 选择【ping】菜单命令，在【IPMaster】对话框下面可以看到网络连通性测试结果，如图 4-20 所示。



图 4-20

4.3.3 局域网监控专家——LanSee

局域网查看工具（LanSee）是一款对局域网上的计算机信息进行查看的工具，LanSee 可以对局域网中的计算机进行扫描，获取计算机的 IP 地址、MAC 地址、计算机名和所在工作组等基本网络信息，然后选择特定的计算机还可以查看其共享资源，同时 LanSee 还集成了网络嗅探功能，可以捕获各种数据包，包括 tcp、udp、icmp 和 arp 等。LanSee 做为一款优秀的局域网监管软件，越

来越受到广大网络管理人员的喜爱，LanSee 扫描计算机和使用共享资源的具体方法如下。

使用 LanSee 局域网监控软件扫描网络计算机的具体操作步骤如下。

01 打开 LanSee 局域网监控软件，在菜单栏中选择【设置】➢【工具选项】菜单命令，如图 4-21 所示。



图 4-21

02 弹出【选项】对话框，在左侧选项列表中选择【搜索计算机】选项，单击【清空】按钮，可以清空默认的 IP 范围，如图 4-22 所示。

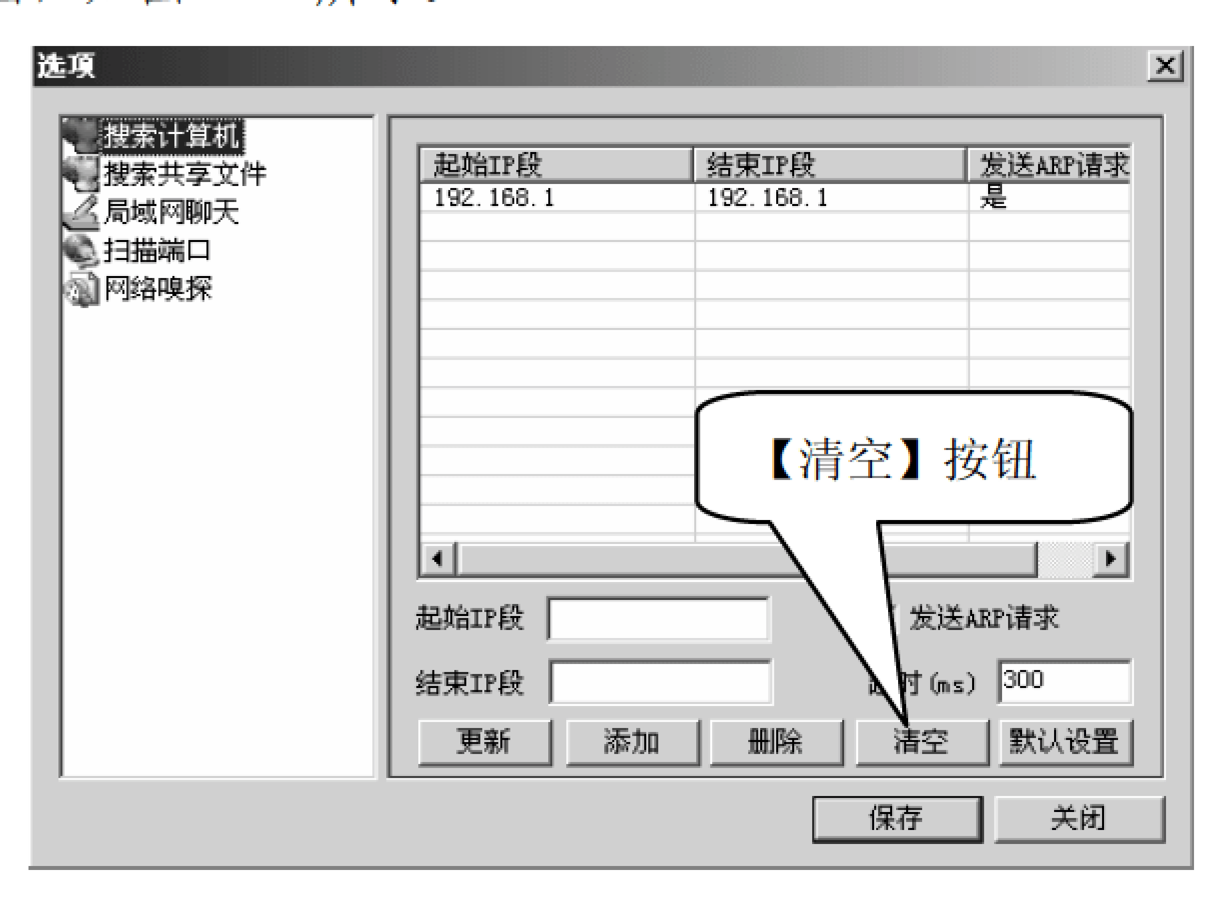


图 4-22

03 单击【添加】按钮，在右侧【起始 IP 段】和【结束 IP 段】文本框中设置要扫描的 IP 范围，单击【保存】按钮，如图 4-23 所示。

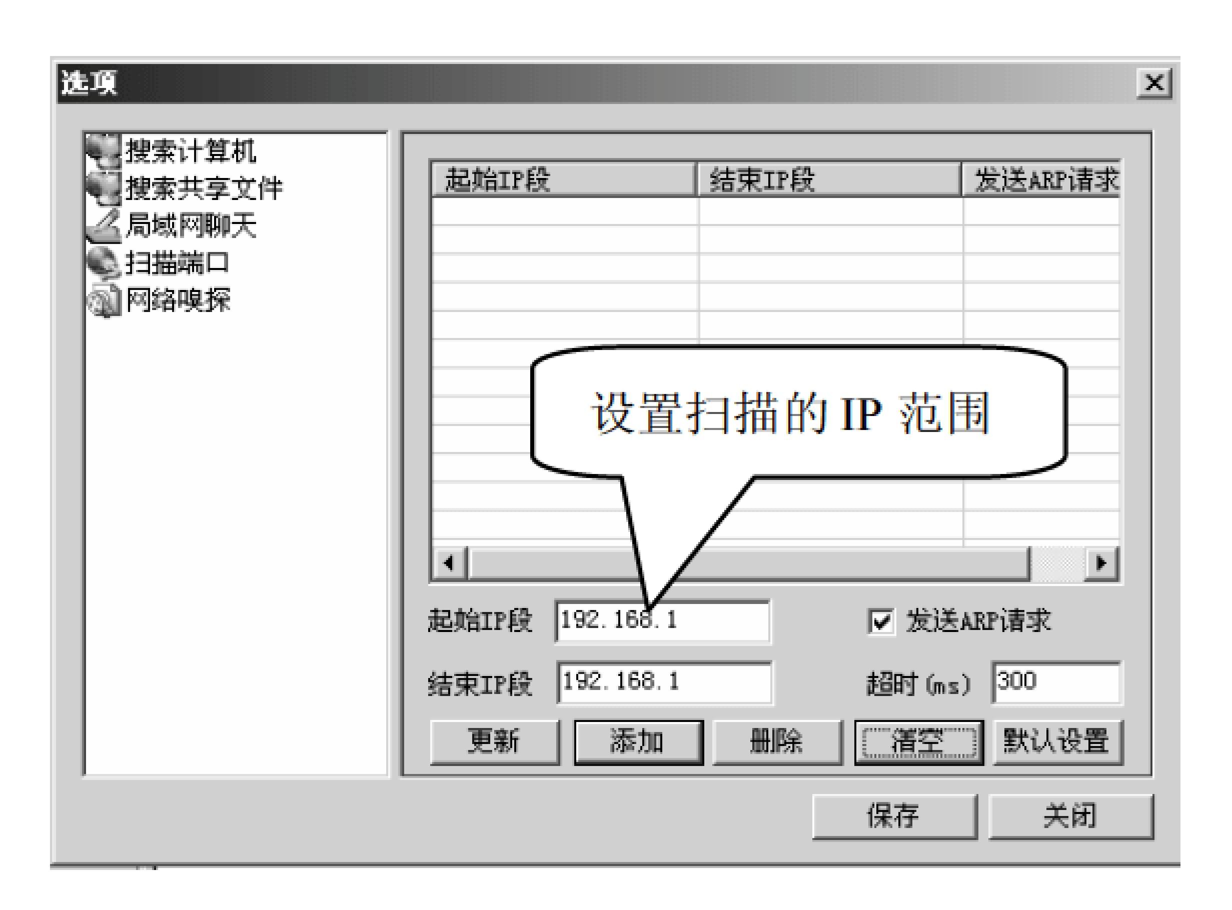


图 4-23

04 返回局域网查看工具（LanSee）程序主界面，在左侧选项列表中单击【搜索工具】选项，在右侧窗格中单击【开始】按钮，开始扫描局域网中计算机的网络基本信息和共享资源信息，如图 4-24 所示。

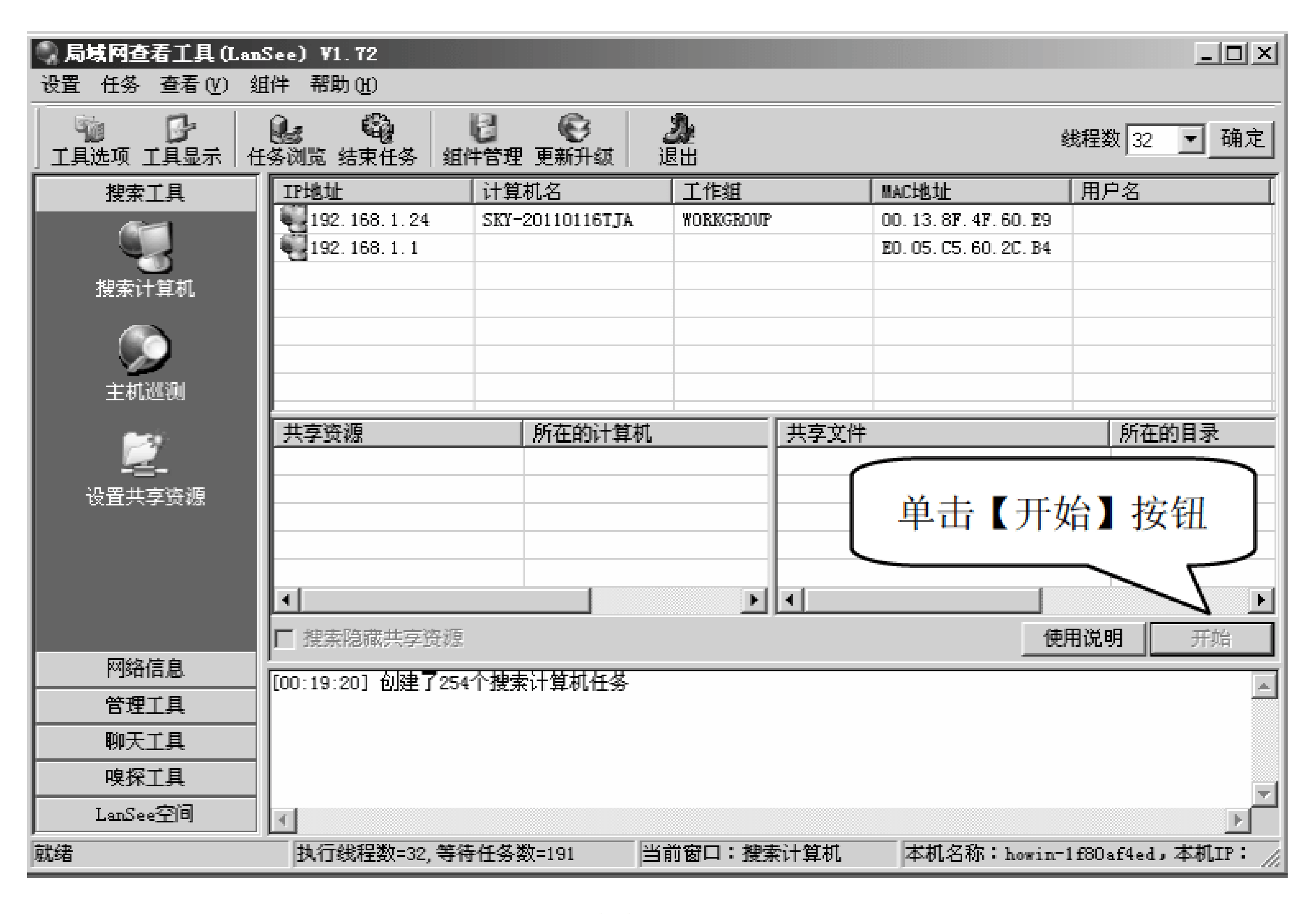


图 4-24

05 扫描结束，如图 4-25 所示可以看到扫描信息，包括局域网计算机的 IP 地址、计算机名、工作组、MAC 地址和共享资源等信息。

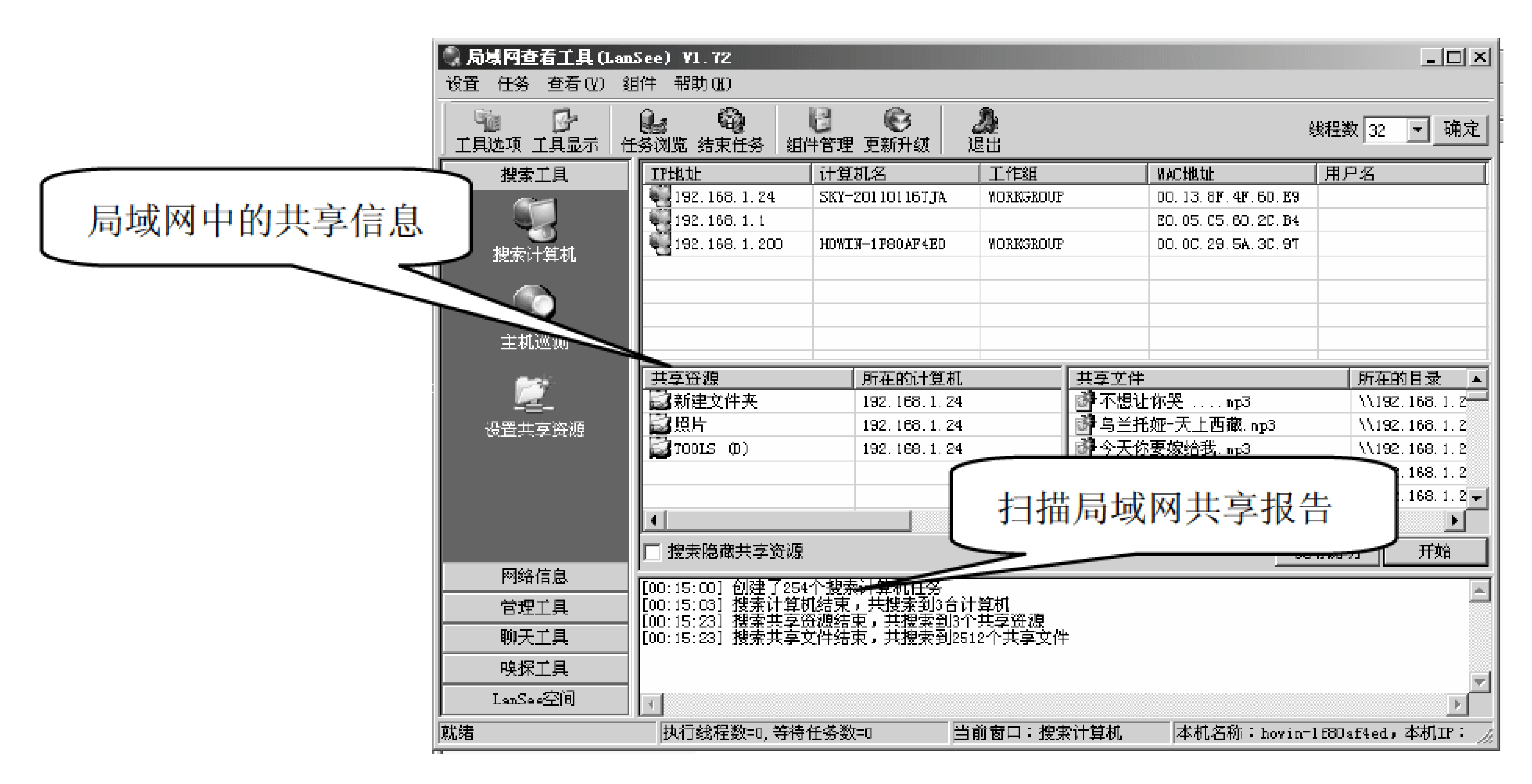


图 4-25

4.3.4 超级扫描工具——SuperScan

对于网络管理员来说，一个功能强大的扫描工具非常重要，在系统被攻击之前扫描出网络的漏洞，是网络管理必备的步骤之一。超级扫描工具 SuperScan 是个功能强大的计算机扫描软件，通过 SuperScan 扫描工具，除了可以获取网络中主机的网络基本信息外，还可以对目标主机开放的端口和服务进行扫描，是网络网管员不可缺少的网络工具。SuperScan 的具体使用步骤如下。

01 打开 SuperScan 工具，首先设置要扫描的 IP 地址范围。在【Hostname/IP】（主机名/IP 地址）文本框中输入本机的 IP 地址，在【Start IP】（起始 IP 地址）文本框中输入要扫描 IP 地址范围的起始地址，在【End IP】（结束 IP 地址）文本框中输入要扫描 IP 地址范围的结束地址，单击【->】按钮将设置的 IP 范围加入扫描范围，单击左下方【▶】按钮，开始扫描，如图 4-26 所示。

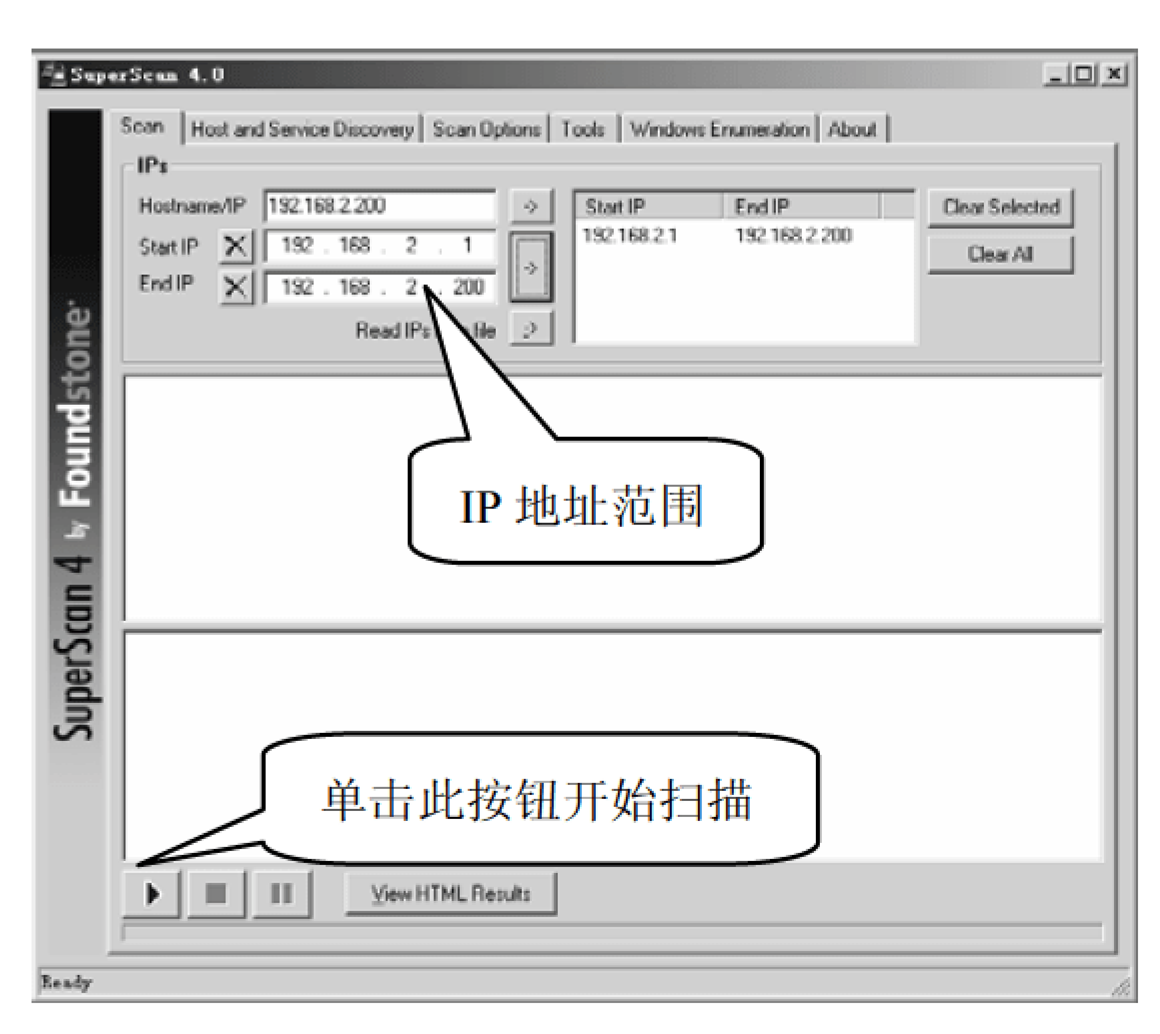


图 4-26

02 SuperScan 扫描工具正在自动扫描，并显示扫描进度，如图 4-27 所示。

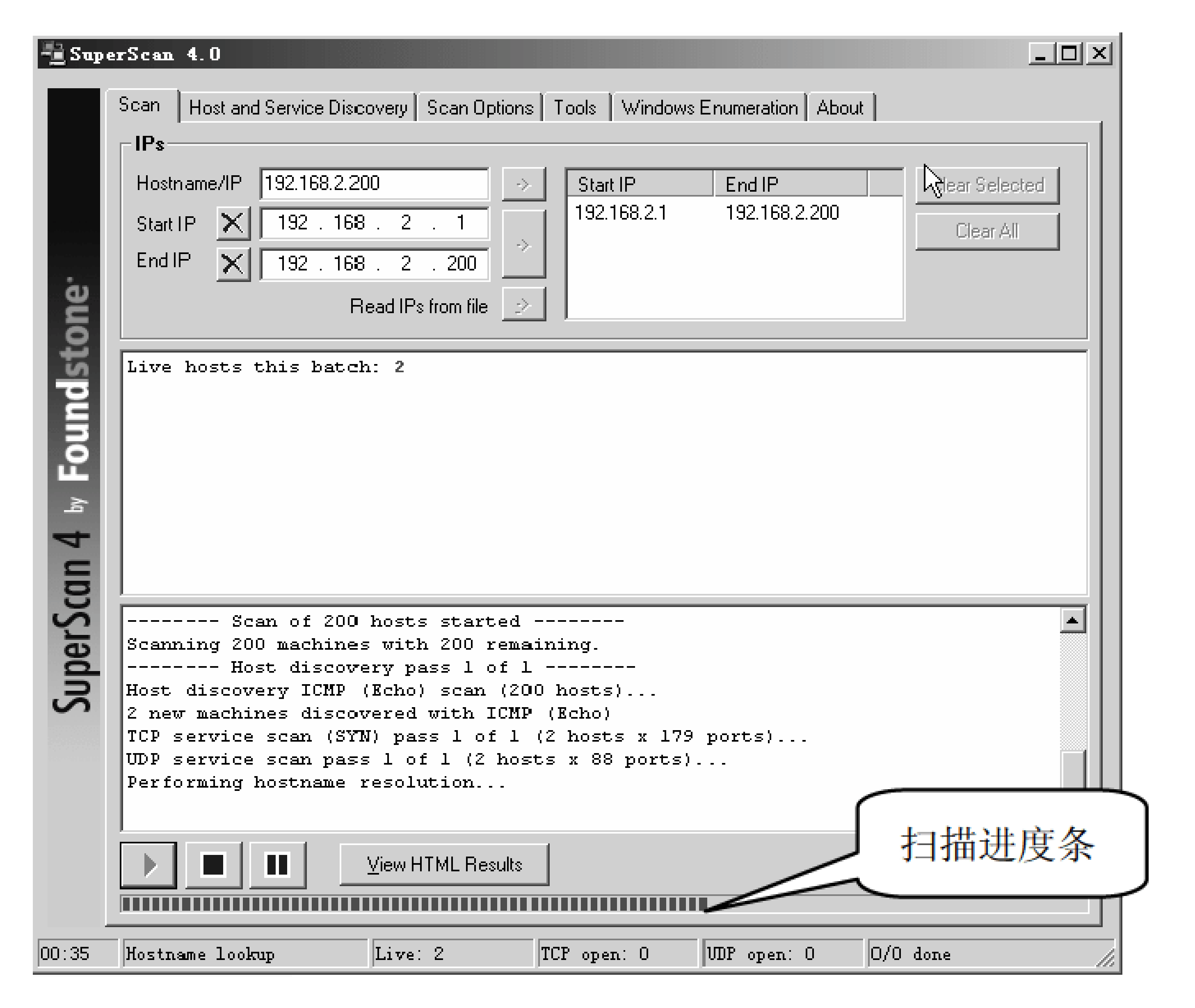


图 4-27

03 SuperScan 扫描完成，并显示扫描结果，如图 4-28 所示。

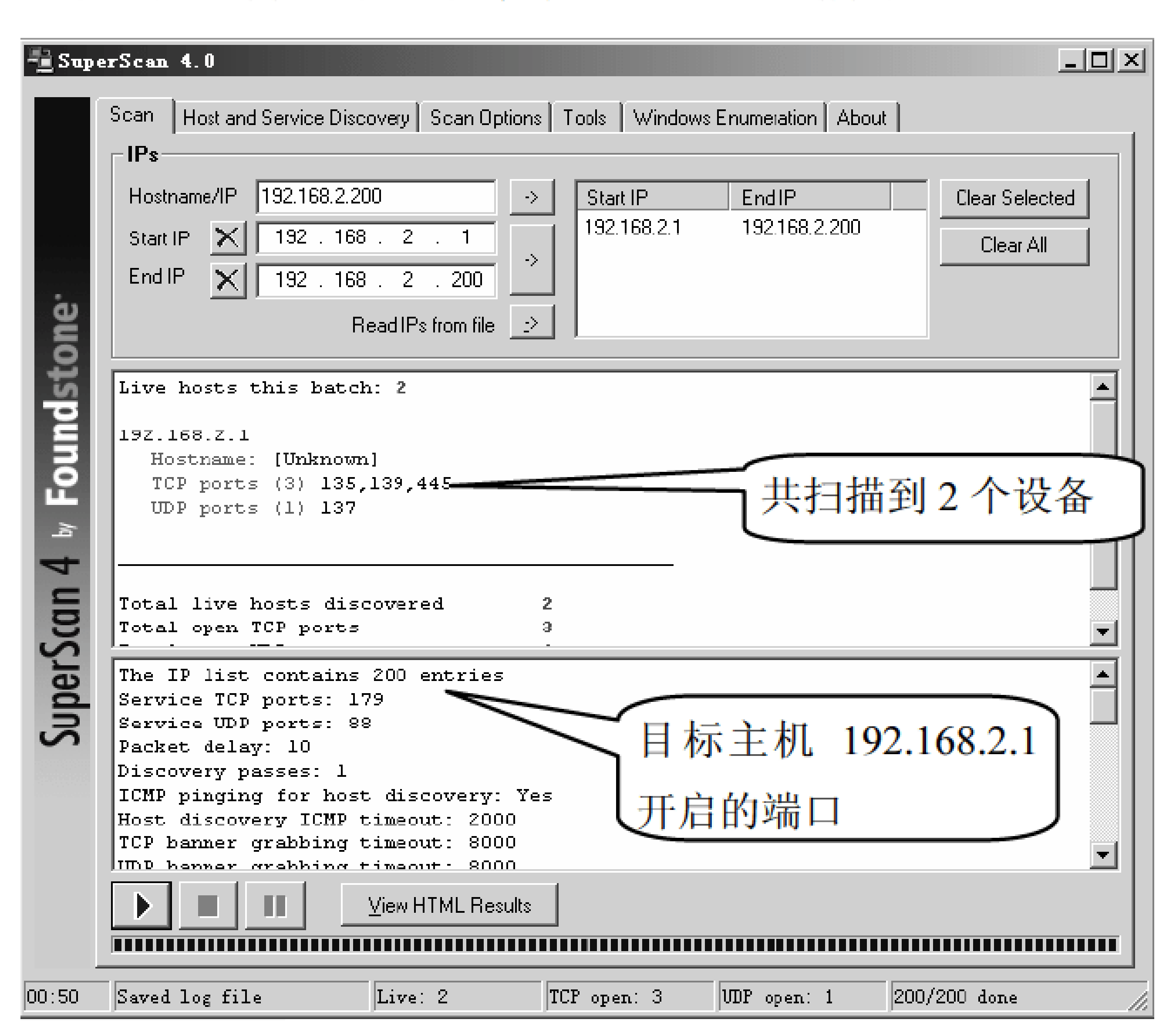


图 4-28

04 单击【View HTML Results】（查看 html 结果）按钮生成 html 格式的扫描报告，如图 4-29 所示。

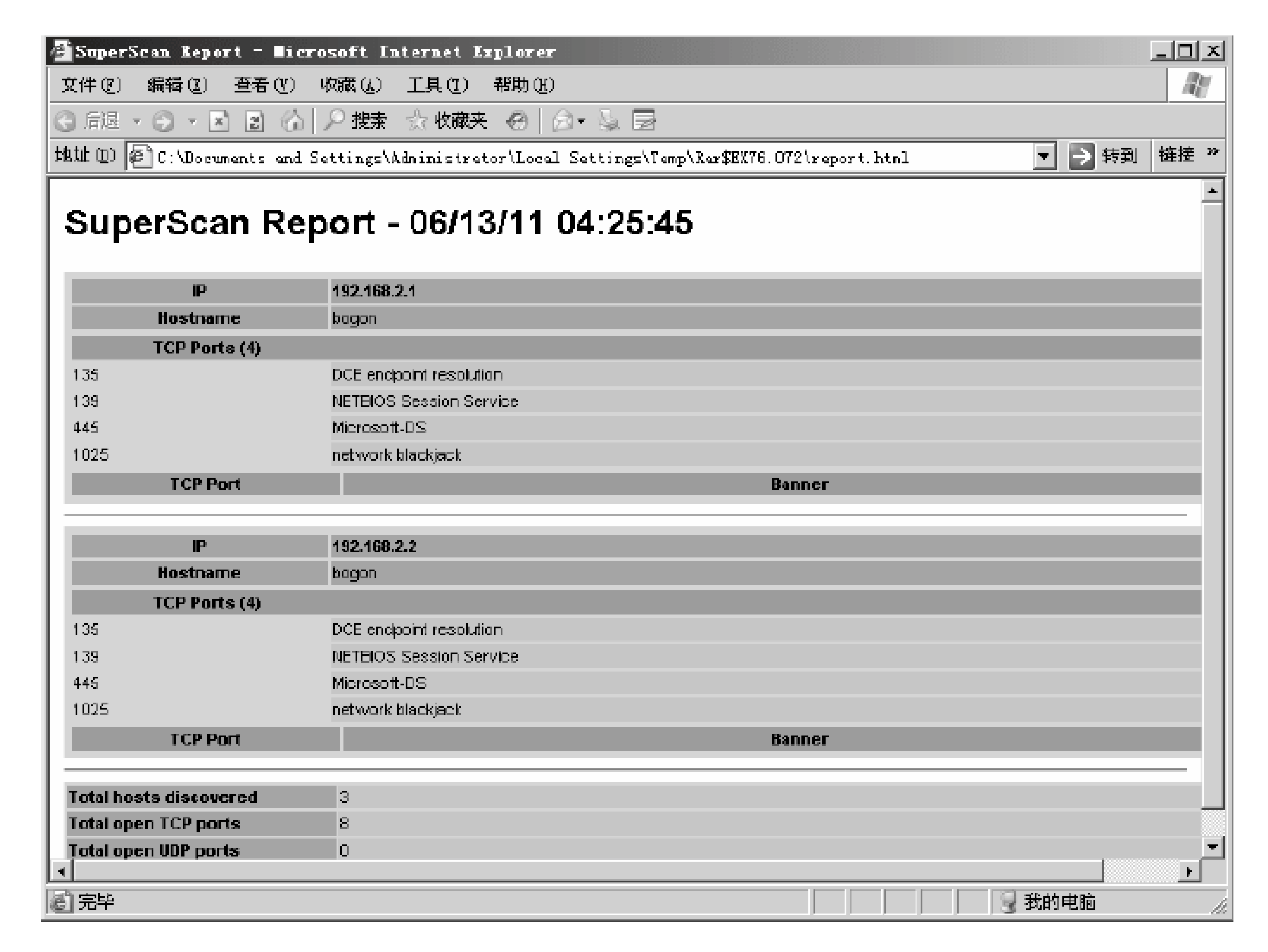


图 4-29

4.4 项目实施 1：生成基本信息库

MAC 扫描器是一款绿色共享软件，主要功能是扫描网络中计算机等设备的 IP 地址、MAC 地址、计算机名称和工作组名称等信息，该软件可以帮助管理员快速的搜集网络基本信息。使用 MAC 扫描器建立基本信息库的具体操作步骤如下。

01 打开 MAC 扫描器，在【IP 范围】文本框中输入要扫描的 IP 地址范围，本案例扫描的 IP 范围是 192.168.1.1 至 192.168.1.255，单击【开始】按钮，如图 4-30 所示。

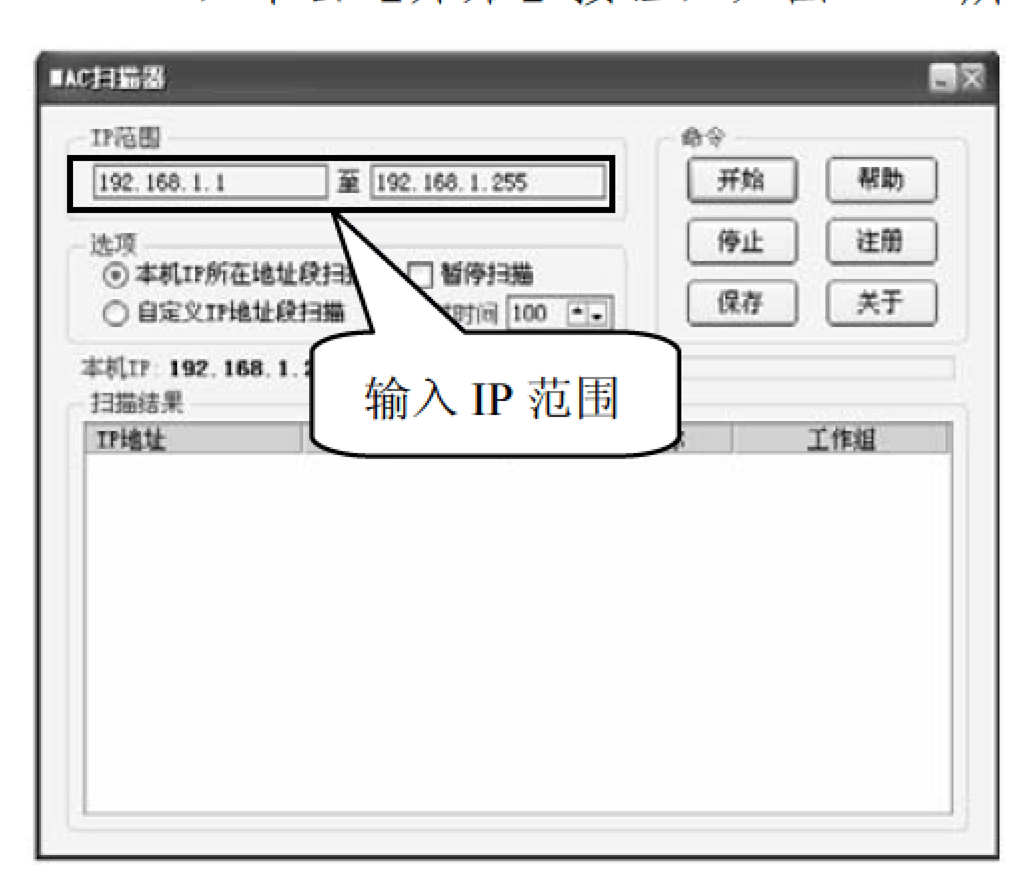


图 4-30

02 MAC 扫描器自动扫描，并显示扫描进度及结果，扫描结束后单击【保存】按钮，如图 4-31 所示。

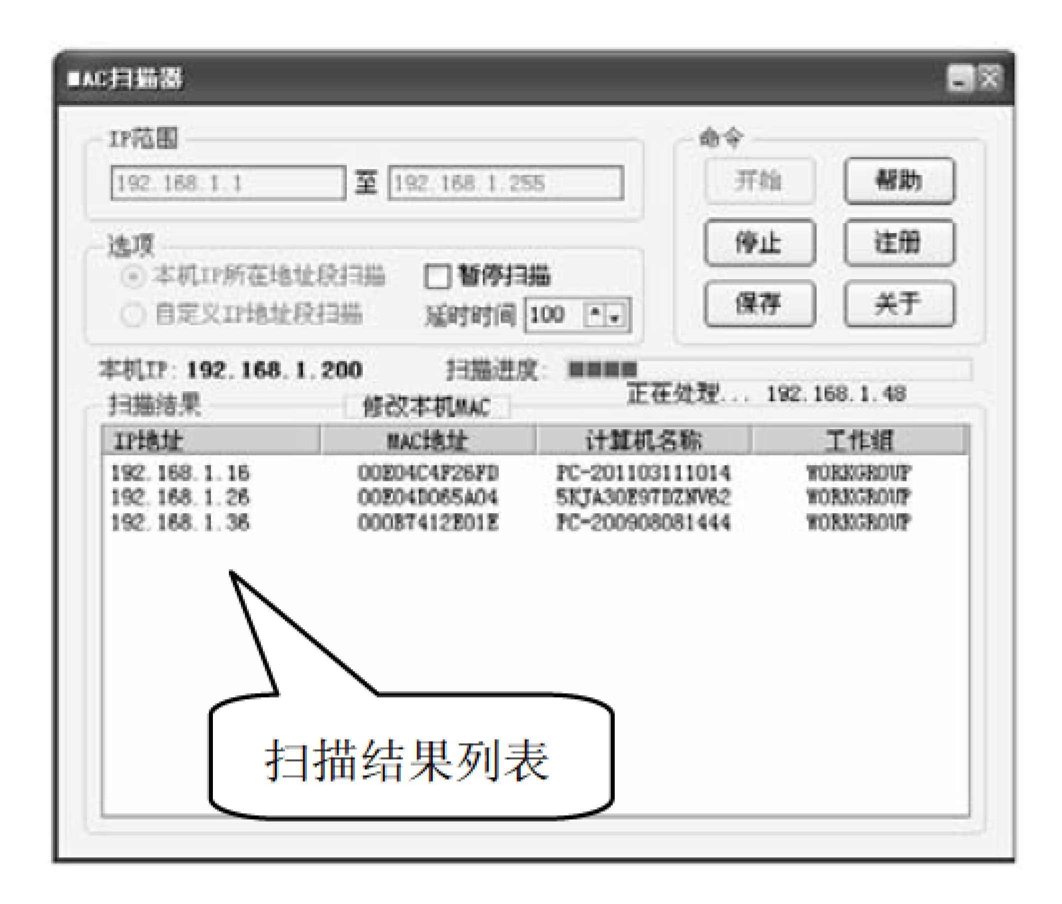


图 4-31

03 弹出【保存】对话框，在【文件名】文本框中输入文件名“ipmac”，保存文件类型为“txt”，单击【保存】按钮，如图 4-32 所示。

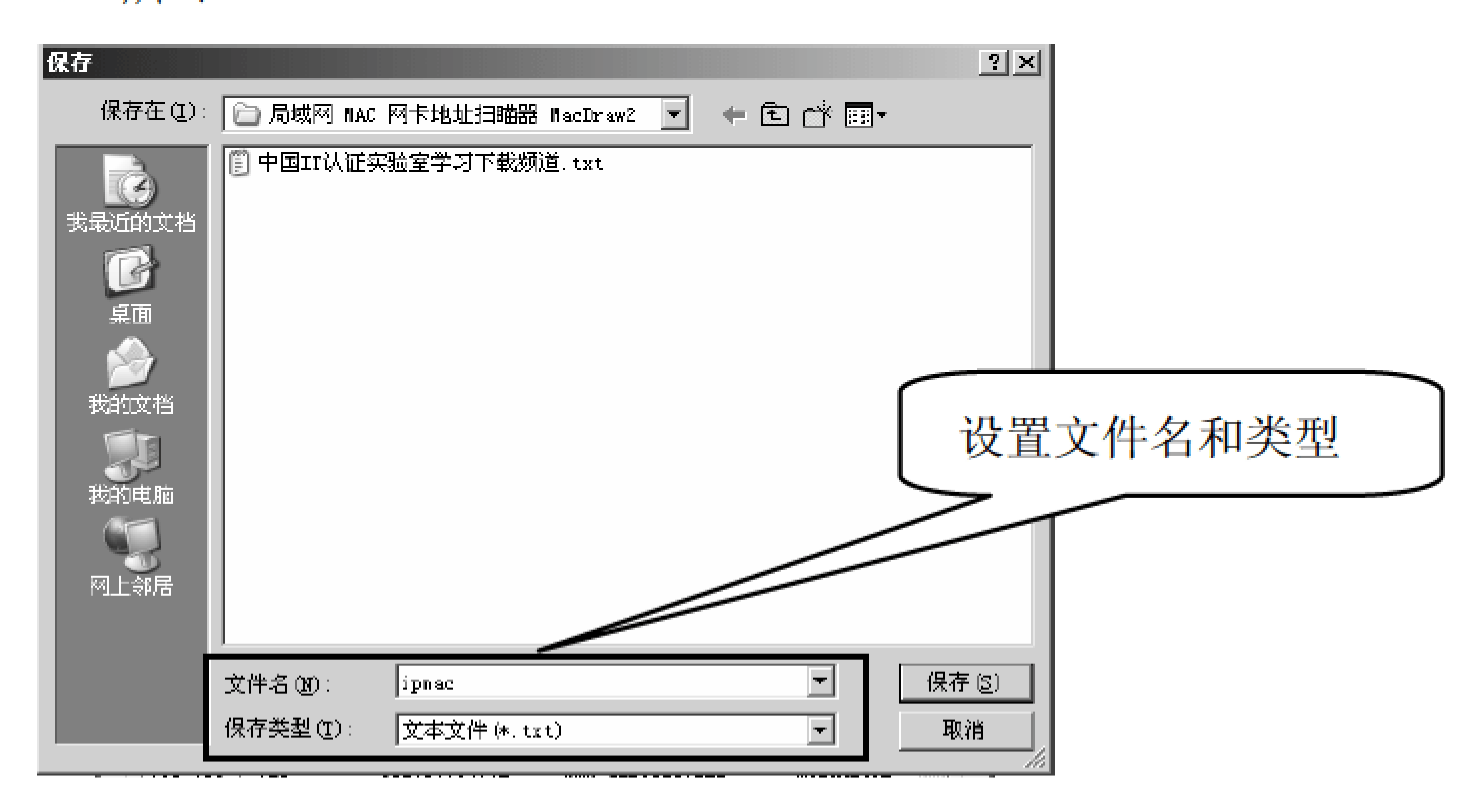


图 4-32

04 打开“ipmac.txt”文件，可以看到搜集到的 IP 地址、MAC 地址、计算机名和工作组名称等网络基本信息，如图 4-33 所示。



图 4-33

05 网络管理员需要将每个 IP 地址的使用者以及设备的物理位置填入该文件以完成基本信息库的建立，如图 4-34 所示。



ipmac.txt - 记事本

IP地址	MAC地址	计算机名称	工作组	员工姓名	设备位置
192.168.1.16	00E04C4F26FD	PC-201123111014	WORKGROUP	王小兵	三楼行政办公室
192.168.1.26	00E04D065A04	5KJA30E97DZNV62	WORKGROUP	聂小帅	二楼人事办公室
192.168.1.36	000B7412E01E	PC-200908081444	WORKGROUP	王红	二楼人事办公室

图 4-34

4.5　项目实施 2：利用基本信息库防止 ARP 欺骗

局域网建立完成后，为了防止 ARP 攻击、ARP 欺骗等局域网常见问题的产生，一般都要求在服务器端对 IP 地址和 MAC 地址进行绑定，这样的话特定的 IP 只能在特定的电脑上使用，既方便管理又能保证局域网的安全。但是面对众多的客户端，无论是在客户端进行 IP 地址和 MAC 地址绑定，还是在服务器端通过网络工具扫描 IP 地址和 MAC 地址进行绑定，对于网络管理员来说都是一个不小的工作量。利用 MS Office Excel 和基本信息库快速进行 IP/MAC 绑定的具体操作步骤如下。

01 启动 MS Office Excel 2003，在菜单栏中选择【数据】➢【导入外部数据】➢【导入数据】菜单命令，选择上文生成的 IP/MAC 映射文本文件，弹出【文本导入向导】对话框，选择【固定宽度】选项，单击【完成】按钮，如图 4-35 所示。



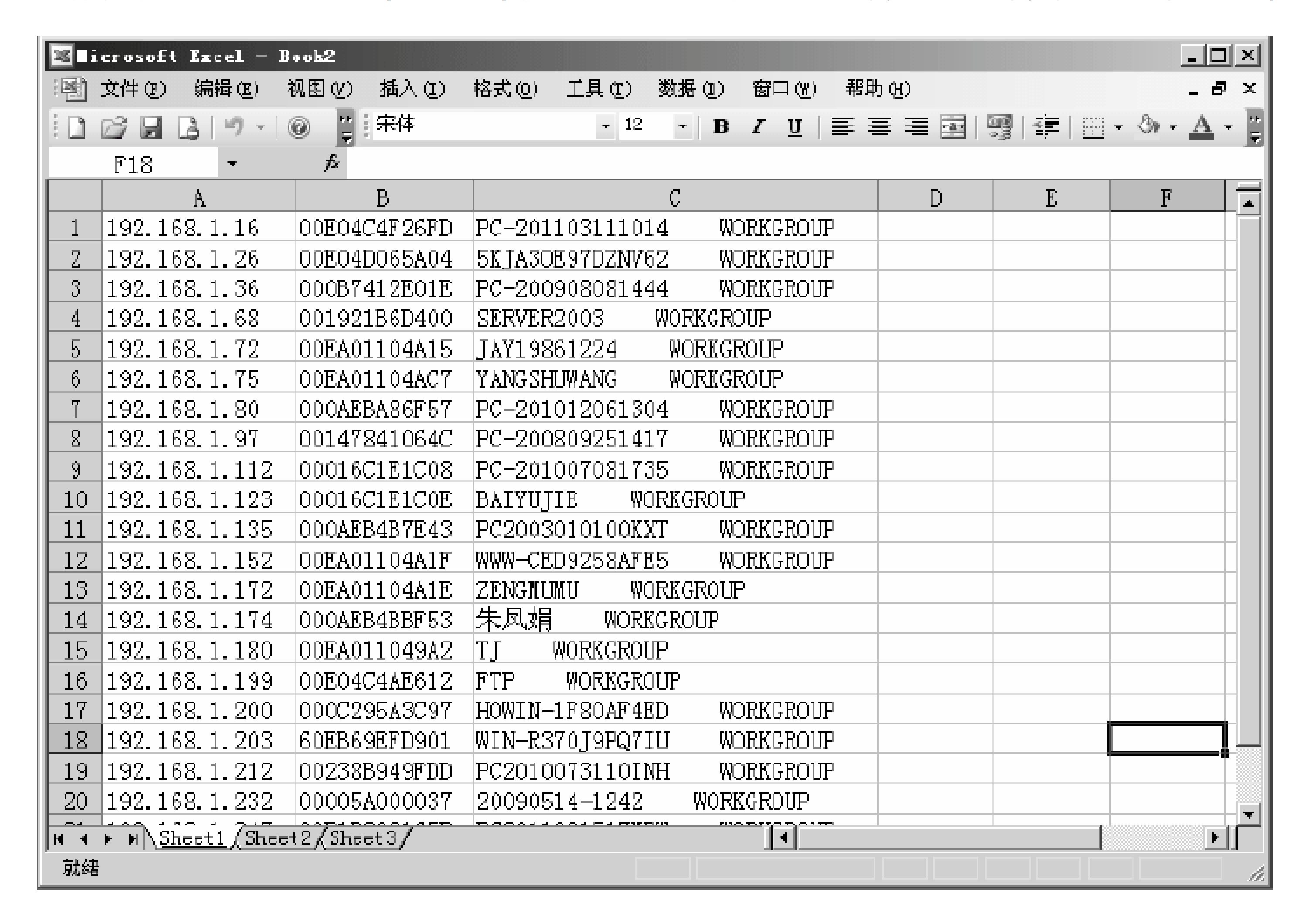
图 4-35

02 弹出【导入数据】对话框，选择【现有工作表】单选按钮，单击【确定】按钮，如图 4-36 所示。



图 4-36

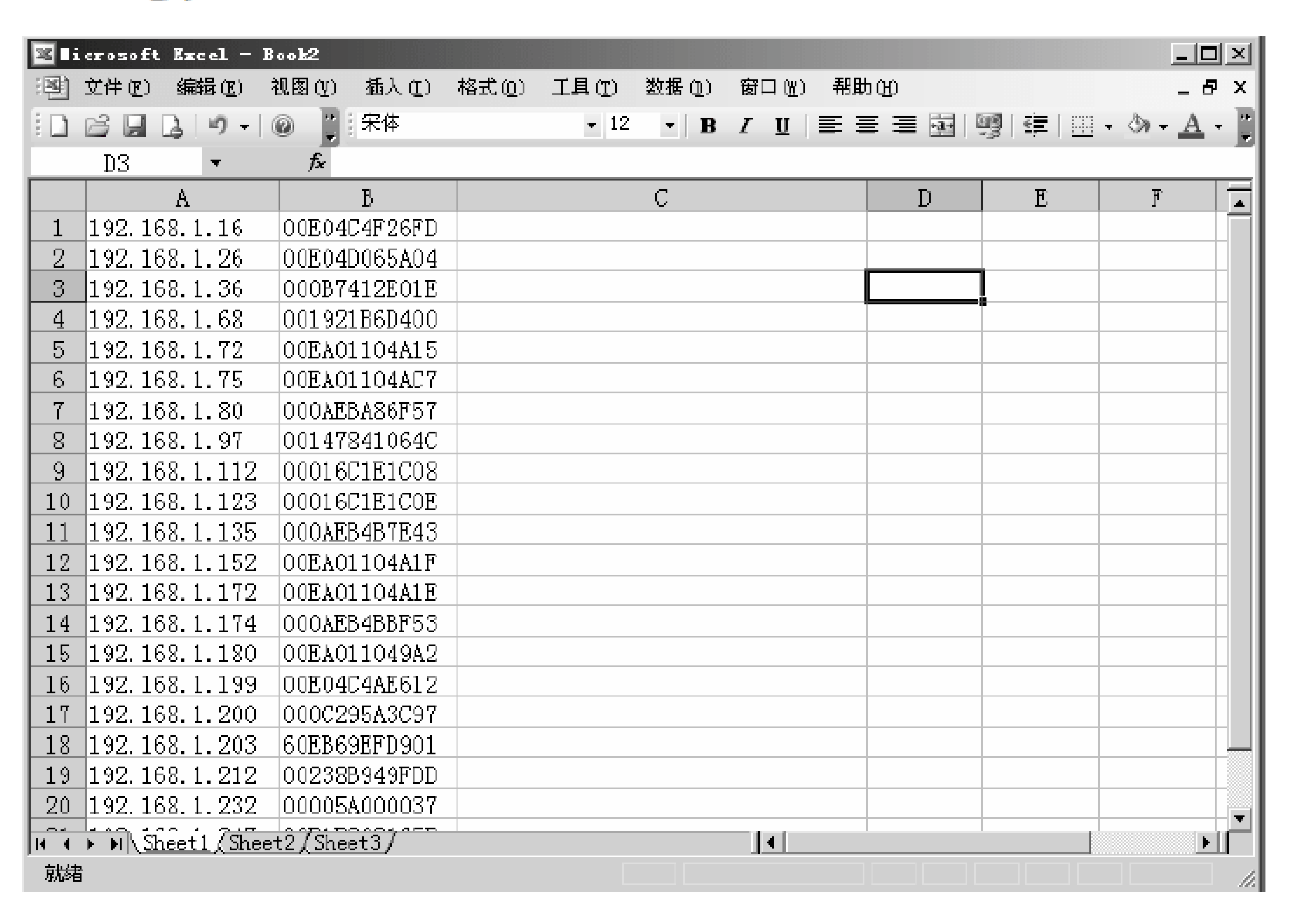
03 如图 4-37 所示，可以看到已经将 IP/MAC 映射文件的文件内容导入到 Excel 表格中。



	A	B	C	D	E	F
1	192.168.1.16	00E04C4F26FD	PC-201103111014　WORKGROUP			
2	192.168.1.26	00E04D065A04	5KJA3OE97DZNV62　WORKGROUP			
3	192.168.1.36	000B7412E01E	PC-200908081444　WORKGROUP			
4	192.168.1.68	001921B6D400	SERVER2003　WORKGROUP			
5	192.168.1.72	00EA01104A15	JAY19861224　WORKGROUP			
6	192.168.1.75	00EA01104AC7	YANGSHUWANG　WORKGROUP			
7	192.168.1.80	000AEBA86F57	PC-201012061304　WORKGROUP			
8	192.168.1.97	00147841064C	PC-200809251417　WORKGROUP			
9	192.168.1.112	00016C1E1C08	PC-201007081735　WORKGROUP			
10	192.168.1.123	00016C1E1C0E	BAIYUJIE　WORKGROUP			
11	192.168.1.135	000AEB4B7E43	PC200301010OKXT　WORKGROUP			
12	192.168.1.152	00EA01104A1F	WWW-CED9258AFE5　WORKGROUP			
13	192.168.1.172	00EA01104A1E	ZENGMUMU　WORKGROUP			
14	192.168.1.174	000AEB4BBF53	朱凤娟　WORKGROUP			
15	192.168.1.180	00EA011049A2	TJ　WORKGROUP			
16	192.168.1.199	00E04C4AE612	FTP　WORKGROUP			
17	192.168.1.200	000C295A3C97	HOWIN-1F80AF4ED　WORKGROUP			
18	192.168.1.203	60EB69EFD901	WIN-R370J9PQ7IU　WORKGROUP			
19	192.168.1.212	00238B949FDD	PC2010073110INH　WORKGROUP			
20	192.168.1.232	00005A000037	20090514-1242　WORKGROUP			

图 4-37

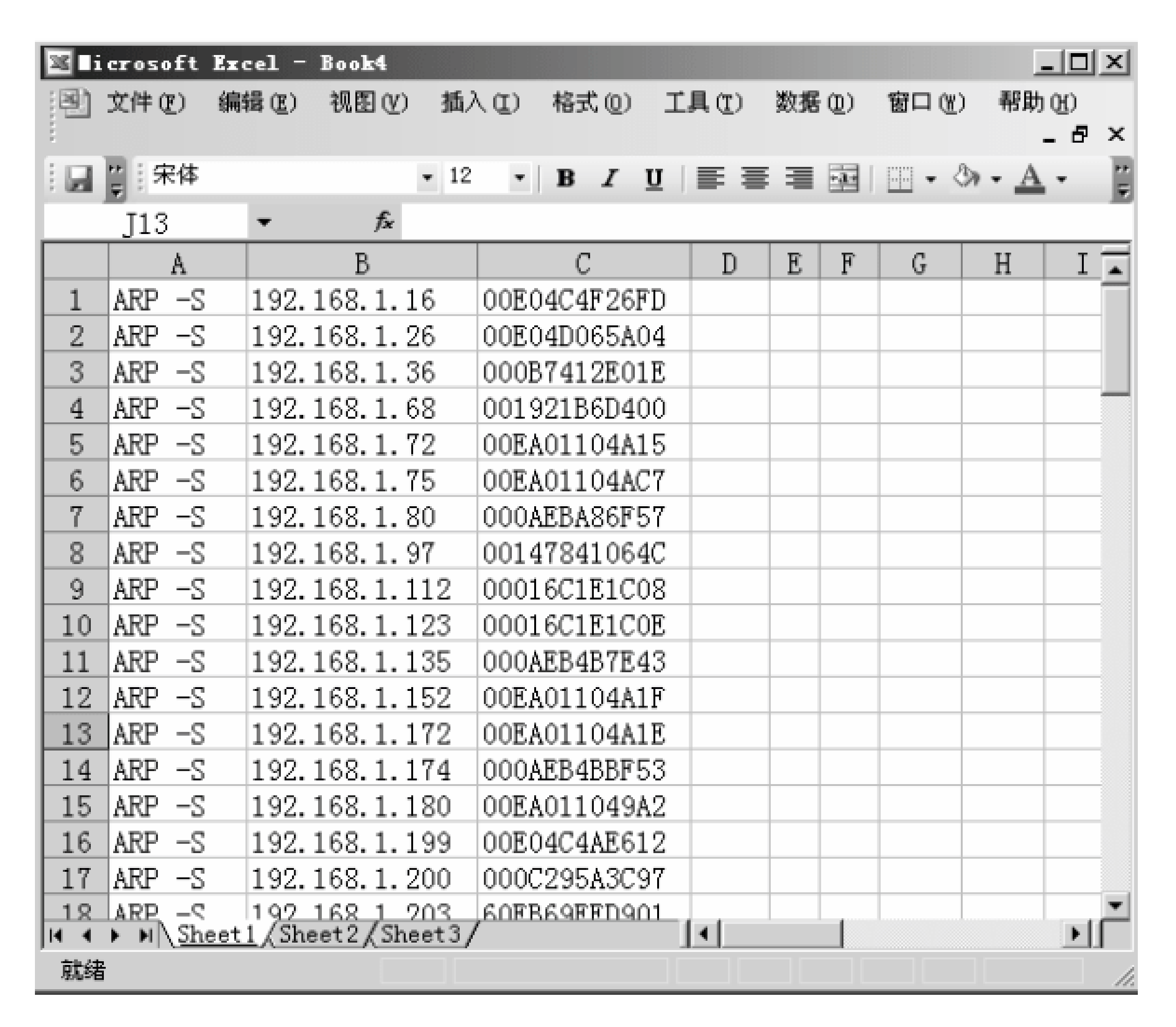
04 如图 4-38 所示，将 Excel 文件中的工作组名称和计算机名称删除掉，此时 Excel 表格中只剩下 IP 地址和 MAC 地址。



	A	B	C	D	E	F
1	192.168.1.16	00E04C4F26FD				
2	192.168.1.26	00E04D065A04				
3	192.168.1.36	000B7412E01E				
4	192.168.1.68	001921B6D400				
5	192.168.1.72	00EA01104A15				
6	192.168.1.75	00EA01104AC7				
7	192.168.1.80	000AEBA86F57				
8	192.168.1.97	00147841064C				
9	192.168.1.112	00016C1E1C08				
10	192.168.1.123	00016C1E1C0E				
11	192.168.1.135	000AEB4B7E43				
12	192.168.1.152	00EA01104A1F				
13	192.168.1.172	00EA01104A1E				
14	192.168.1.174	000AEB4BBF53				
15	192.168.1.180	00EA011049A2				
16	192.168.1.199	00E04C4AE612				
17	192.168.1.200	000C295A3C97				
18	192.168.1.203	60EB69EFD901				
19	192.168.1.212	00238B949FDD				
20	192.168.1.232	00005A000037				

图 4-38

05 在 Excel 表格中 A 列前插入一列，然后在新插入的这一列单元格内输入绑定 MAC 地址的命令和参数“ARP -S”，如图 4-39 所示。



	A	B	C	D	E	F	G	H	I
1	ARP -S	192.168.1.16	00E04C4F26FD						
2	ARP -S	192.168.1.26	00E04D065A04						
3	ARP -S	192.168.1.36	000B7412E01E						
4	ARP -S	192.168.1.68	001921B6D400						
5	ARP -S	192.168.1.72	00EA01104A15						
6	ARP -S	192.168.1.75	00EA01104AC7						
7	ARP -S	192.168.1.80	000AEBA86F57						
8	ARP -S	192.168.1.97	00147841064C						
9	ARP -S	192.168.1.112	00016C1E1C08						
10	ARP -S	192.168.1.123	00016C1E1C0E						
11	ARP -S	192.168.1.135	000AEB4B7E43						
12	ARP -S	192.168.1.152	00EA01104A1F						
13	ARP -S	192.168.1.172	00EA01104A1E						
14	ARP -S	192.168.1.174	000AEB4BBF53						
15	ARP -S	192.168.1.180	00EA011049A2						
16	ARP -S	192.168.1.199	00E04C4AE612						
17	ARP -S	192.168.1.200	000C295A3C97						
18	ARP -S	192.168.1.203	60EB69EFD901						

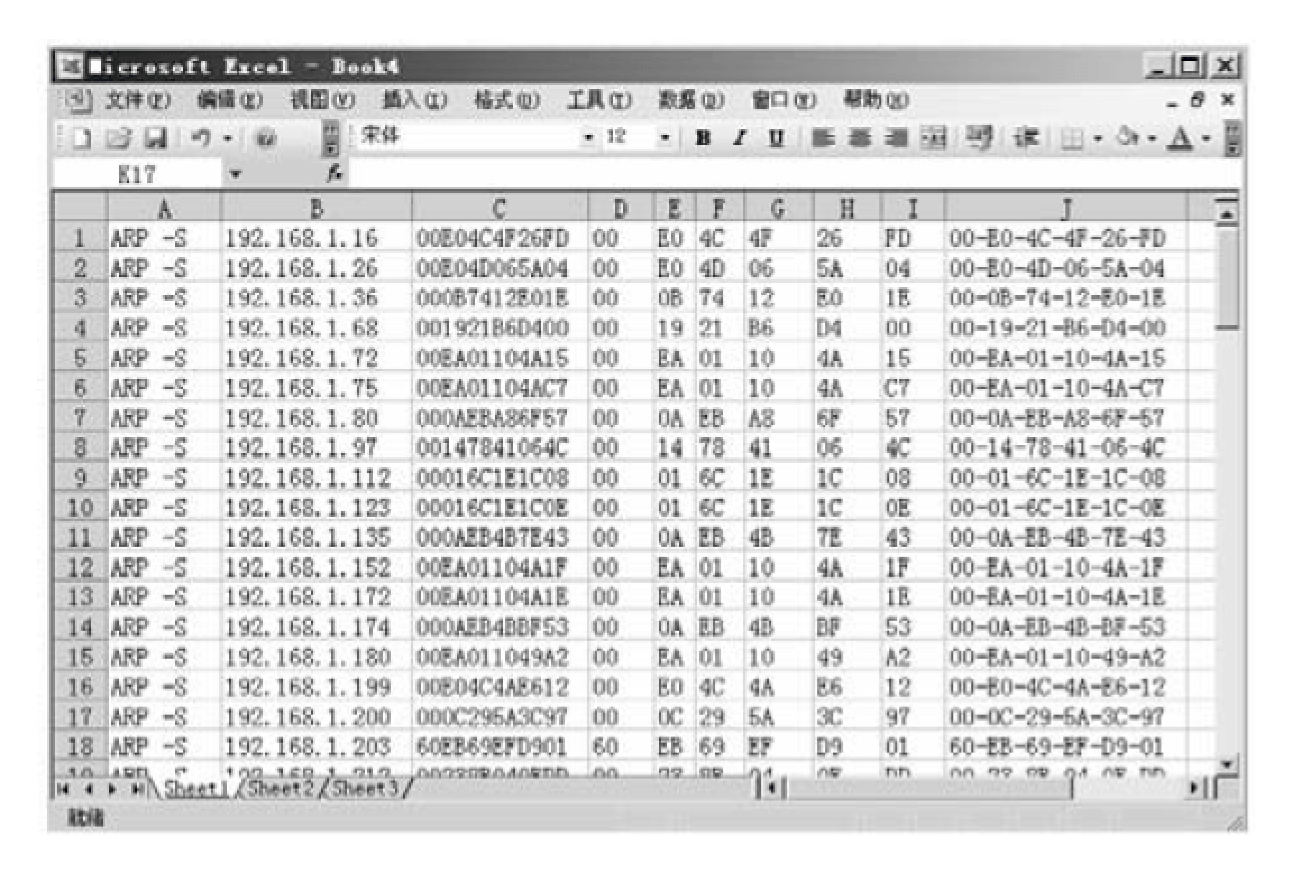
图 4-39

06 利用字符串函数分割 12 位 MAC 地址为两两一组，操作方法为：在 D1 单元格输入“=left(C1,2)”，在 E1 单元格输入“=mid(C1,3,2)”，在 F1 单元格输入“=mid(C1,5,2)”，在 G1 单元格输入“=mid(C1,7,2)”，在 H1 单元格输入“=mid(C1,9,2)”，在 I1 单元格输入“=right(C1, 2)”，然后利用填充法将其他单元格进行输入，得到如图 4-40 所示结果。

	A	B	C	D	E	F	G	H	I
1	ARP -S	192.168.1.16	00E04C4F26FD	00	E0	4C	4F	26	FD
2	ARP -S	192.168.1.26	00E04D065A04	00	E0	4D	06	5A	04
3	ARP -S	192.168.1.36	000B7412E01E	00	0B	74	12	E0	1E
4	ARP -S	192.168.1.68	001921B6D400	00	19	21	B6	D4	00
5	ARP -S	192.168.1.72	00EA01104A15	00	EA	01	10	4A	15
6	ARP -S	192.168.1.75	00EA01104AC7	00	EA	01	10	4A	C7
7	ARP -S	192.168.1.80	000AEBA86F57	00	0A	EB	A8	6F	57
8	ARP -S	192.168.1.97	00147841064C	00	14	78	41	06	4C
9	ARP -S	192.168.1.112	00016C1E1C08	00	01	6C	1E	1C	08
10	ARP -S	192.168.1.123	00016C1E1C0E	00	01	6C	1E	1C	0E
11	ARP -S	192.168.1.135	000AEB4B7E43	00	0A	EB	4B	7E	43
12	ARP -S	192.168.1.152	00EA01104A1F	00	EA	01	10	4A	1F
13	ARP -S	192.168.1.172	00EA01104A1E	00	EA	01	10	4A	1E
14	ARP -S	192.168.1.174	000AEB4BBF53	00	0A	EB	4B	BF	53
15	ARP -S	192.168.1.180	00EA011049A2	00	EA	01	10	49	A2
16	ARP -S	192.168.1.199	00E04C4AE612	00	E0	4C	4A	E6	12
17	ARP -S	192.168.1.200	000C295A3C97	00	0C	29	5A	3C	97
18	ARP -S	192.168.1.203	60EB69EFD901	60	EB	69	EF	D9	01

图 4-40

07 在 J1 单元格内把 D1~I1 单元格的内容合并起来，中间用减号分隔。操作方法为：在 J1 内输入“=D1&"-"&E1&"-"&F1&"-"&G1&"-"&H1&"-"&I1”，然后使用填充法依次填充 J 列单元格，结果如图 4-41 所示。



Microsoft Excel - Book4

	A	B	C	D	E	F	G	H	I	J
1	ARP -S	192.168.1.16	00E04C4F26FD	00	E0	4C	4F	26	FD	00-E0-4C-4F-26-FD
2	ARP -S	192.168.1.26	00E04D065A04	00	E0	4D	06	5A	04	00-E0-4D-06-5A-04
3	ARP -S	192.168.1.36	000B7412E01E	00	0B	74	12	E0	1E	00-0B-74-12-E0-1E
4	ARP -S	192.168.1.68	001921B6D400	00	19	21	B6	D4	00	00-19-21-B6-D4-00
5	ARP -S	192.168.1.72	00EA01104A15	00	EA	01	10	4A	15	00-EA-01-10-4A-15
6	ARP -S	192.168.1.75	00EA01104AC7	00	EA	01	10	4A	C7	00-EA-01-10-4A-C7
7	ARP -S	192.168.1.80	000AEBA86F57	00	0A	EB	A8	6F	57	00-0A-EB-A8-6F-57
8	ARP -S	192.168.1.97	00147841064C	00	14	78	41	06	4C	00-14-78-41-06-4C
9	ARP -S	192.168.1.112	00016C1E1C08	00	01	6C	1E	1C	08	00-01-6C-1E-1C-08
10	ARP -S	192.168.1.123	00016C1E1C0E	00	01	6C	1E	1C	0E	00-01-6C-1E-1C-0E
11	ARP -S	192.168.1.135	000AEB4B7E43	00	0A	EB	4B	7E	43	00-0A-EB-4B-7E-43
12	ARP -S	192.168.1.152	00EA01104A1F	00	EA	01	10	4A	1F	00-EA-01-10-4A-1F
13	ARP -S	192.168.1.172	00EA01104A1E	00	EA	01	10	4A	1E	00-EA-01-10-4A-1E
14	ARP -S	192.168.1.174	000AEB4BBF53	00	0A	EB	4B	BF	53	00-0A-EB-4B-BF-53
15	ARP -S	192.168.1.180	00EA011049A2	00	EA	01	10	49	A2	00-EA-01-10-49-A2
16	ARP -S	192.168.1.199	00E04C4AE612	00	E0	4C	4A	E6	12	00-E0-4C-4A-E6-12
17	ARP -S	192.168.1.200	000C295A3C97	00	0C	29	5A	3C	97	00-0C-29-5A-3C-97
18	ARP -S	192.168.1.203	60EB69EFD901	60	EB	69	EF	D9	01	60-EB-69-EF-D9-01

图 4-41

08 将 C 列至 I 列所有数据进行隐藏。选中 C 列至 I 列的所有数据，然后右击，选择【隐藏】选项，如图 4-42 所示。

Microsoft Excel - Book4

	A	B	J	K	L
1	ARP -S	192.168.1.16	00-E0-4C-4F-26-FD		
2	ARP -S	192.168.1.26	00-E0-4D-06-5A-04		
3	ARP -S	192.168.1.36	00-0B-74-12-E0-1E		
4	ARP -S	192.168.1.68	00-19-21-B6-D4-00		
5	ARP -S	192.168.1.72	00-EA-01-10-4A-15		
6	ARP -S	192.168.1.75	00-EA-01-10-4A-C7		
7	ARP -S	192.168.1.80	00-0A-EB-A8-6F-57		
8	ARP -S	192.168.1.97	00-14-78-41-06-4C		
9	ARP -S	192.168.1.112	00-01-6C-1E-1C-08		
10	ARP -S	192.168.1.123	00-01-6C-1E-1C-0E		
11	ARP -S	192.168.1.135	00-0A-EB-4B-7E-43		
12	ARP -S	192.168.1.152	00-EA-01-10-4A-1F		
13	ARP -S	192.168.1.172	00-EA-01-10-4A-1E		
14	ARP -S	192.168.1.174	00-0A-EB-4B-BF-53		
15	ARP -S	192.168.1.180	00-EA-01-10-49-A2		
16	ARP -S	192.168.1.199	00-E0-4C-4A-E6-12		
17	ARP -S	192.168.1.200	00-0C-29-5A-3C-97		

图 4-42

09 选择【文件】菜单中的【保存】选项，将数据进行保存，命名为“IP/MAC 映射表”，如图 4-43 所示。



图 4-43

10 打开上述步骤制作的“IP/MAC 映射表”，将里面的内容复制在一个文本文档中，如图 4-44 所示。

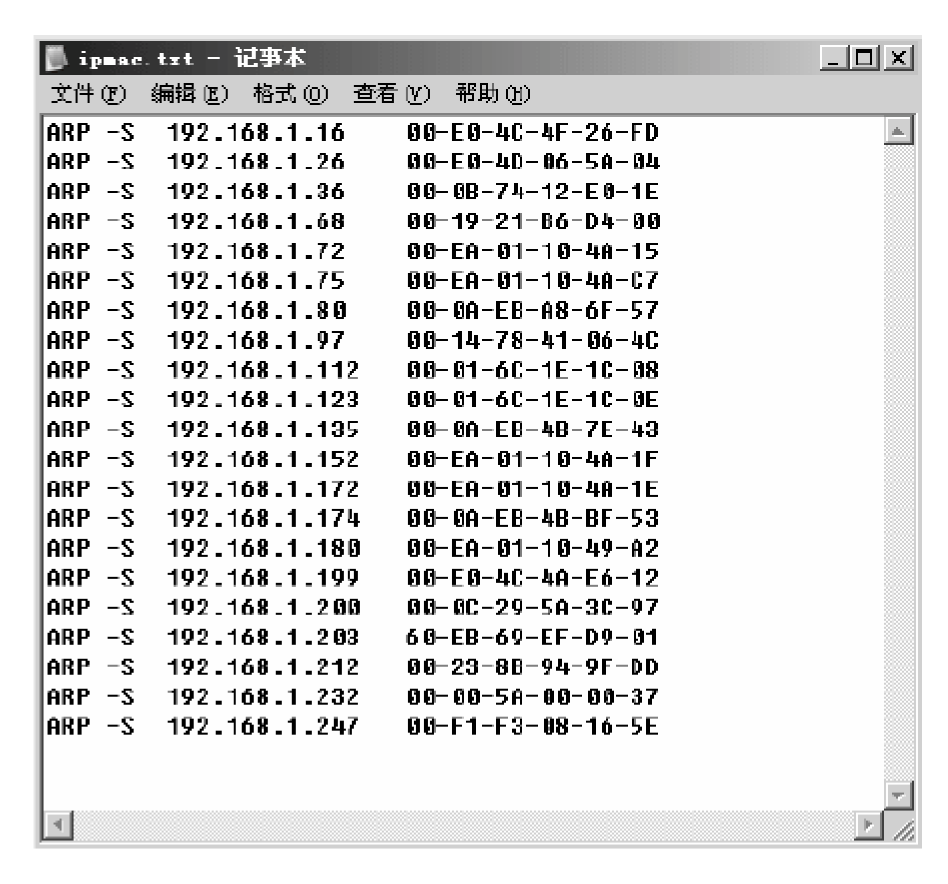


图 4-44

11 选择【文件】菜单中的【另存为】选项，弹出【另存为】对话框，将文本文档保存为“ipmac.bat”，如图 4-45 所示。



图 4-45

12 在服务器上直接运行这个批处理文件，可以进行 IP 地址和 MAC 地址的绑定，如图 4-46 所示。

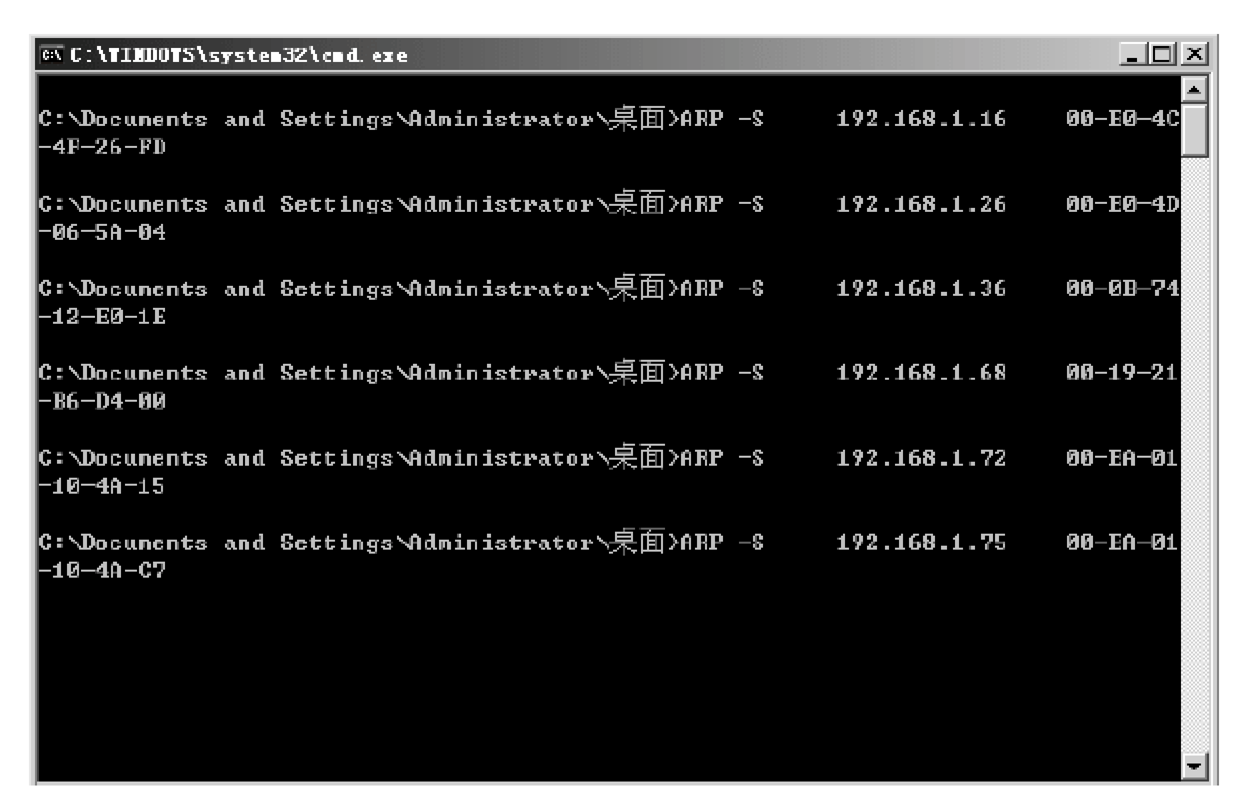


图 4-46

4.6　专家答疑

（1）在使用 IPMaster、LanSee 等工具的时候，操作步骤是正确的，为什么却扫描不到信息？

答：可以从两个方面考虑出现这一现象的原因。其一，扫描工具所在的计算机网络连接是否正常，可以通过网络测试工具，测试网络连接状态；其二，是否安装了 Winpcap 驱动包，该驱动包主要是为 Windows 应用程序提供访问网络底层的能力，大部分的网络管理工具都需要用到该驱动包。

（2）我已经在服务器上做了 IP/MAC 地址绑定，可网络中还存在 ARP 攻击？如何解决？

答：从理论上说在出口服务器上进行 IP/MAC 绑定，可以更好的对局域网进行管理，有效地防止 IP 欺骗和 ARP 欺骗等问题，但是对于局域网内部的此类问题还需要在每个计算机上进行 IP/MAC 绑定，当然没有一种办法是万能的，对于局域网内部的问题还需要计算机使用者的配合，避免在局域网中使用 p2p 攻击软件，及时升级杀毒软件，防止计算机中毒。

第 5 章　搭建网络管理平台

随着各公司企业网络环境的不断完善，网络规模也在逐步扩大，面对越来越多的网络设备，越来越复杂的网络拓扑结构，传统的管理方式已经显得有些笨拙，如何更有效、更直观地实施网络管理，成为了不少技术人员关注的话题。

伴随这些问题，先后出现了很多网络管理工具，其中网络管理平台是网络环境管理中最系统、最直观的工具之一。通过网络管理平台，可以直观地查看到当前网络的动态拓扑结构，实时查看所有网络设备的性能状态，以帮助网络管理员实施网络管理。

5.1　网络管理平台介绍

随着网络技术的发展，网络管理工具层出不穷，但是很多工具在查看网络运行状态上比较被动，网络出现故障时不能通过工具及时表现出来，具体的网络故障点也要运用工具去测试。而网络管理平台却可以动态显示全网的链接状态，一旦出现设备故障或链接故障，都会及时通过网络管理平台显现出来，大大提高了故障的发现和解决效率。因此，搭建可靠的网络管理平台成为了企业网络管理过程中必不可少的内容。

5.1.1　什么是网络管理平台

网络管理平台也可称作网络运维管理系统。对于运营商的网络环境管理，一般都称作网络运维管理，所以大多数厂商都会使用网络运维管理系统这个名字。

网络管理平台不单单是一个网络管理软件的安装。首先，要使用 SNMP 等网络管理协议搭建一套可管理的网络环境，这个在第 2 章中已经做了介绍；其次，要在网络中指定的网络管理设备上安装网络管理平台软件。满足以上两点，才算是一套完整的网络管理平台系统。

通过网络管理协议，网络管理平台可以获取所有网络设备、服务器、主机的运行状态及其性能参数。但是网络管理平台的产品比较繁杂，功能也有所差异。

具体来说，网络管理平台的主要功能有以下几个方面。

1. 真实动态的网络拓扑管理

利用网络管理平台，可以自动生成全网的物理拓扑结构，动态实时反映网络布线信息，设备运行状态及链路的流量变化情况等，帮助网络管理员一目了然地掌控整个网络的实时运行状态。

如图 5-1 所示为使用 Spiceworks 软件获取的网络拓扑图。

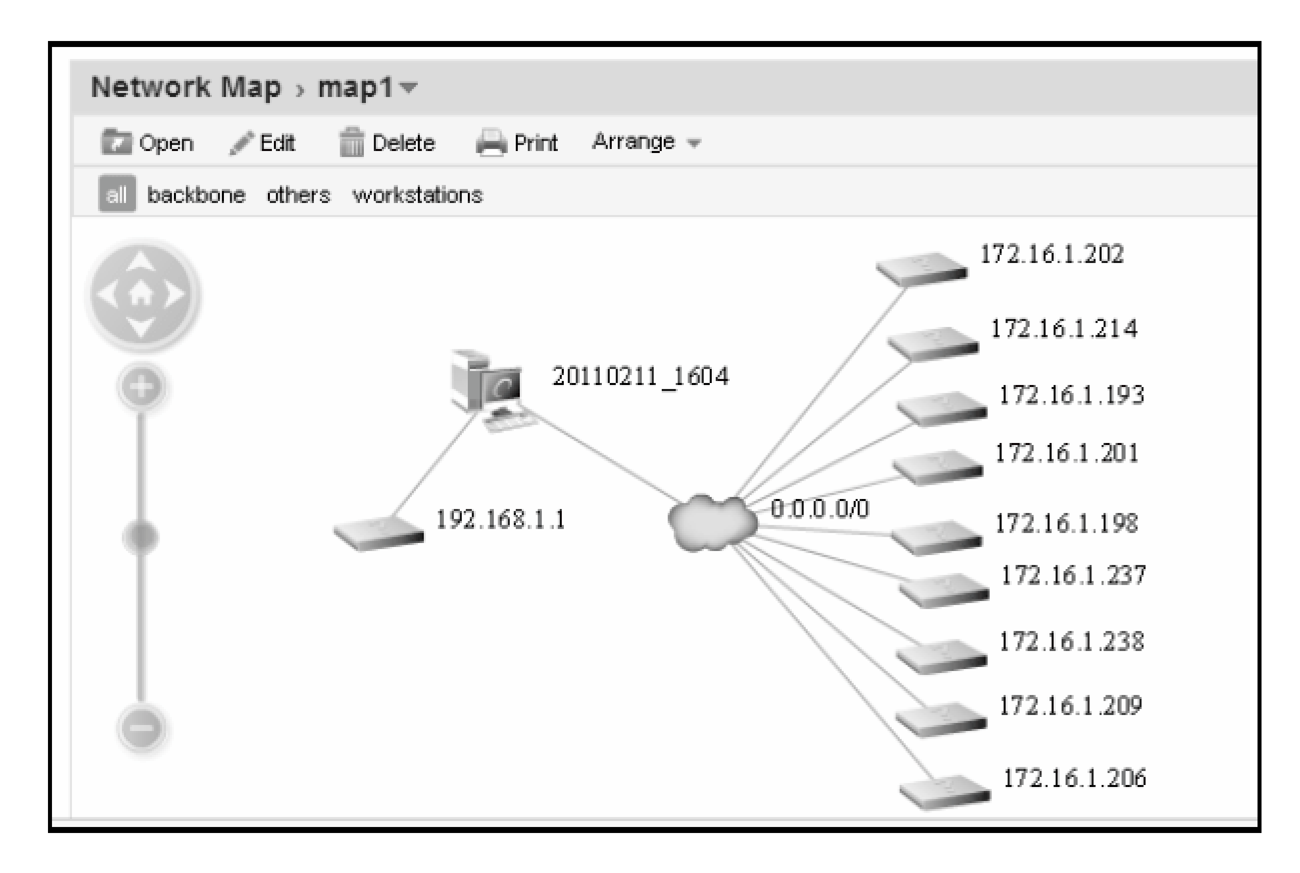


图 5-1

2. 层次化分明的统一管理

当网络的管理区域相当庞大时，通过网络管理平台可以实现分层、跨地域的管理。上层网络管理员可以概括地看到各大区域的链接状况，也可以细化地查看某一区域内查地拓扑结构。

3. 多厂商设备的全面管理

设备管理是网络平台管理的核心。大多数网络管理平台都只是 SNMP 网络管理协议，只要设备运行了 SNMP 管理协议，就可以被网络管理平台监控，和设备的厂商没有直接关系。

4. 全面完善的告警系统

解决网络故障的效率，在网络管理过程中至关重要。当故障发生后再去修复，必然后造成损失。如果在网络运行刚出现异常时就能被发现，故障就会在造成损失前被解决。因此很多网络管理平台都会设置告警系统，对于网络设备、网络链接的流量异常、性能异常等均可设置告警。

如图 5-2 所示为 Spiceworks 软件的告警配置页面。

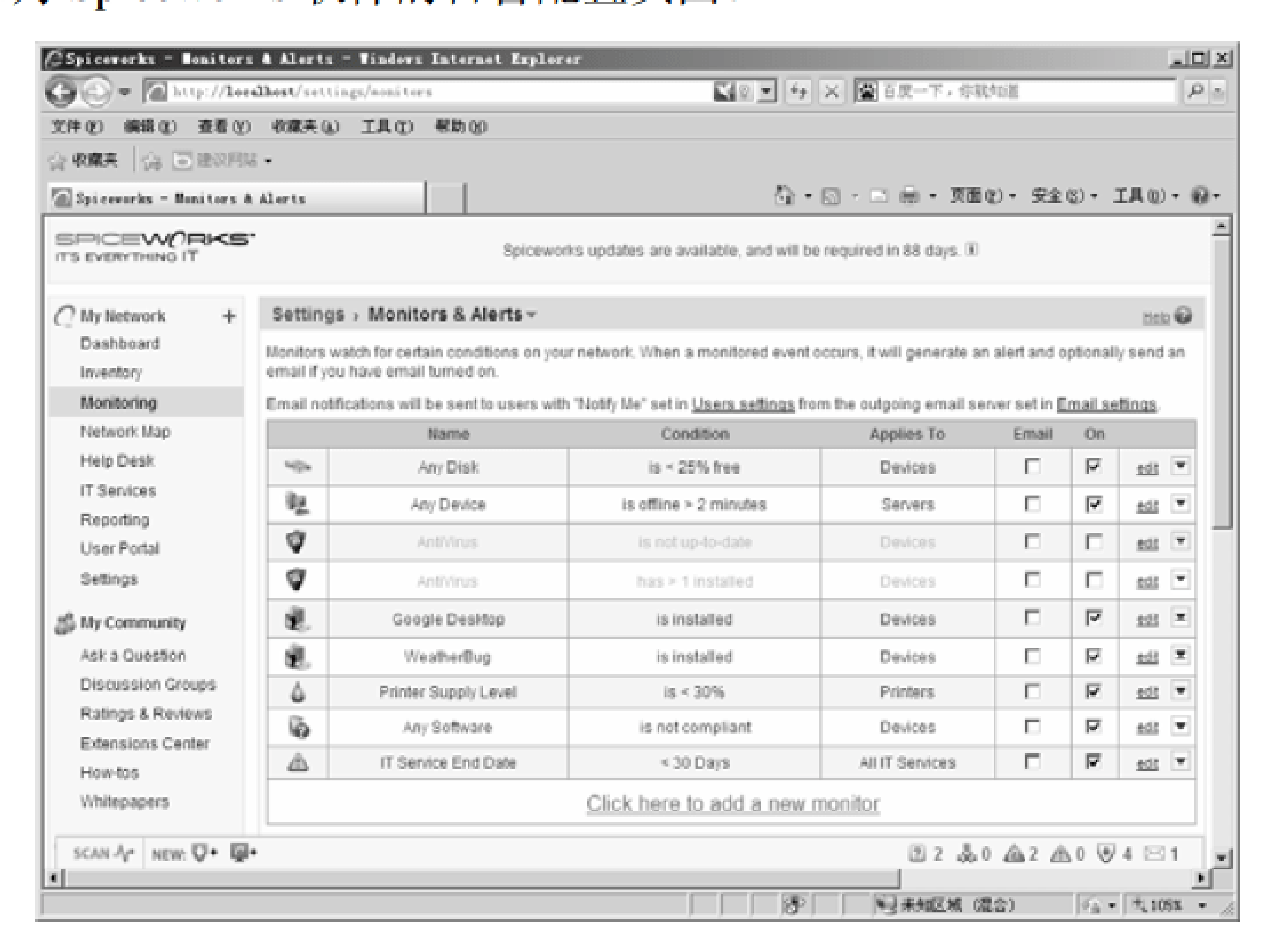


图 5-2

5. 全网地址定位的安全管理

网络管理平台可以实现全网 IP 定位、MAC 定位，结合网络安全技术进行安全隐患的排查，捕捉地址盗用及非法设备移动等。

6. 系统的报表查询功能

通过对网络的管理、监控，网络管理平台可以产生各类报表，包括各类性能指标的统计、均量、趋势等。利用这些报表信息，可以有效地分析网络性能状态。

如图 5-3 所示为 WhatsUp Gold 软件的事件查看报表。

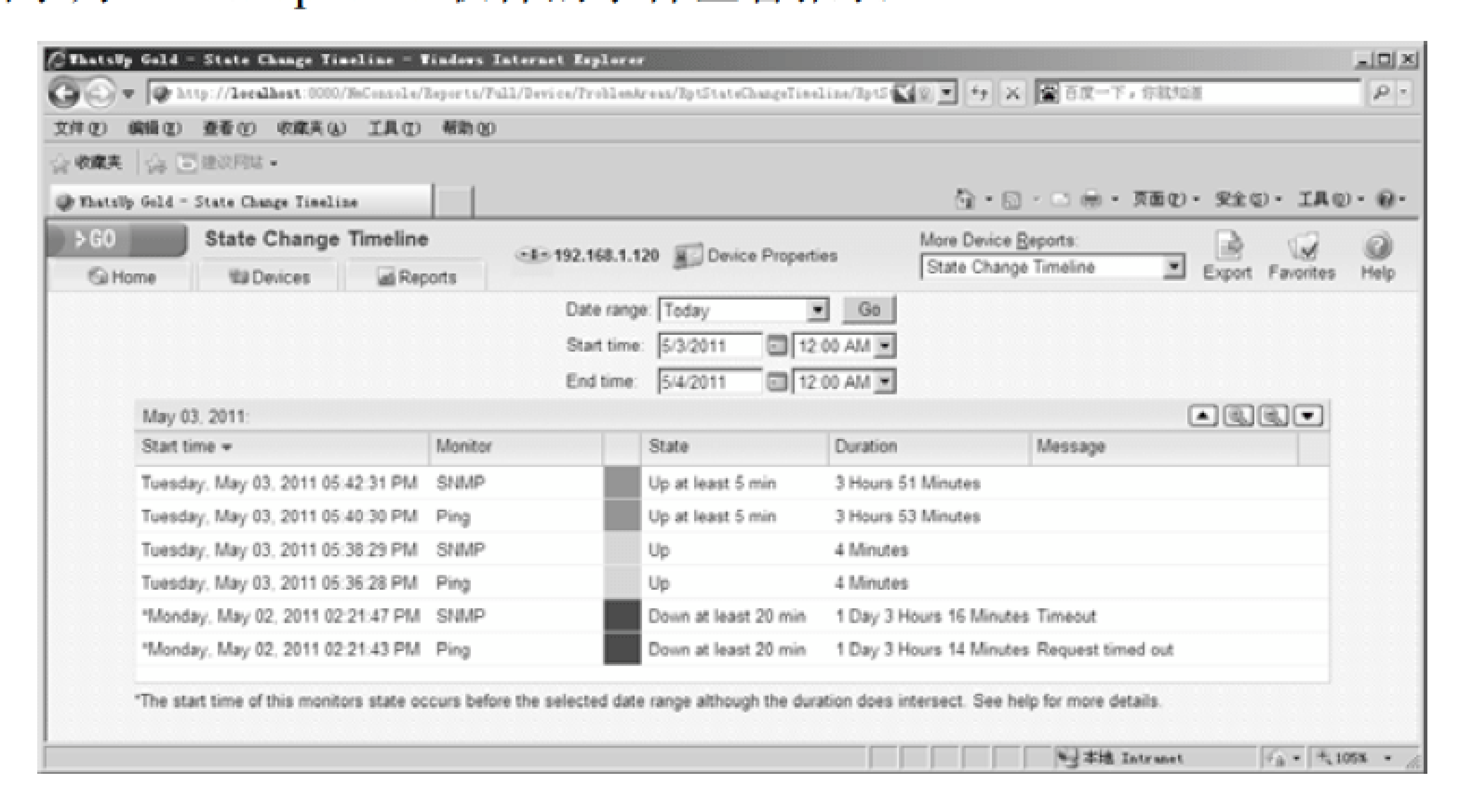


图 5-3

7. 异常数据流分析

部分网络管理平台还支持网络流量的抓捕、分析功能，通过数据流量分析，可以发现黑客扫描、病毒扩散、网络攻击、大流量下载等网络问题，并快速地找到问题源。

5.1.2 主流网络管理平台产品

市场上的网络管理平台产品非常多，主流网络产品有以下几个。

1. Spiceworks

Spiceworks 是一款针对中小型企业的网络设备管理和监控软件。它由广告商提供支持，是一款免费软件。根据 Spiceworks 公司的介绍，这款软件适合雇员人数在 250 人以下的中小型企业，其产品功能和特点都是针对这一市场而定制的。

如图 5-4 所示为 Spiceworks 网络管理平台的主页面。

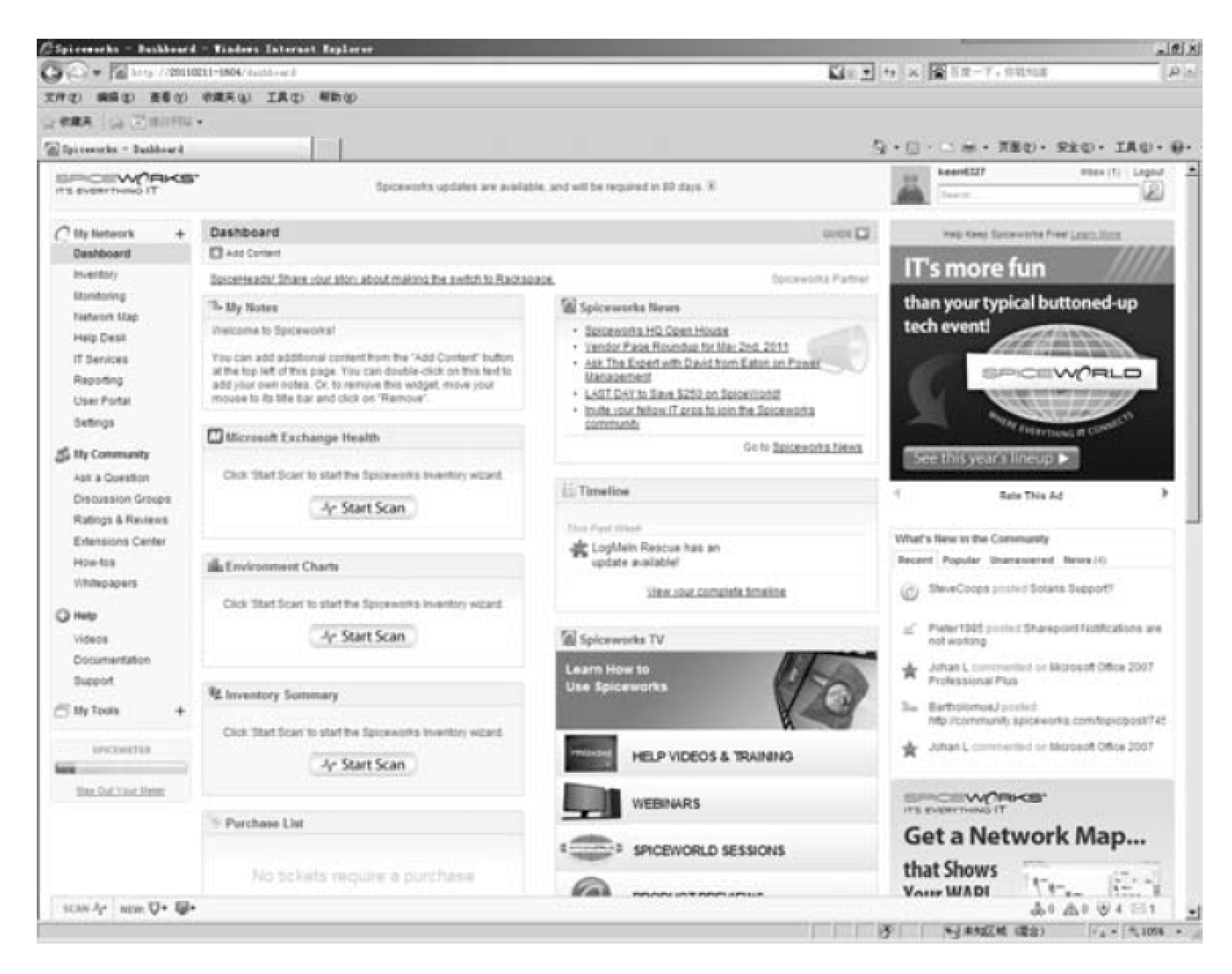


图 5-4

2. WhatsUp Gold

WhatsUp Gold 提供完整、易用的监控机制，全方位监控应用服务与网络设备，能协助 IT 管理人员将网管信息转变成可阅读的商业信息。WhatsUp Gold 能主动监控所有关键网络设备与应用服务，因而减少影响业务运作的停机问题，避免严重损失。WhatsUp Gold 因具有操作容易、快速布署、扩充性强、高投资报酬率等优势而独树一帜。

如图 5-5 所示为 WhatsUp Gold 网络管理平台查看网络设备的 Web 页面。

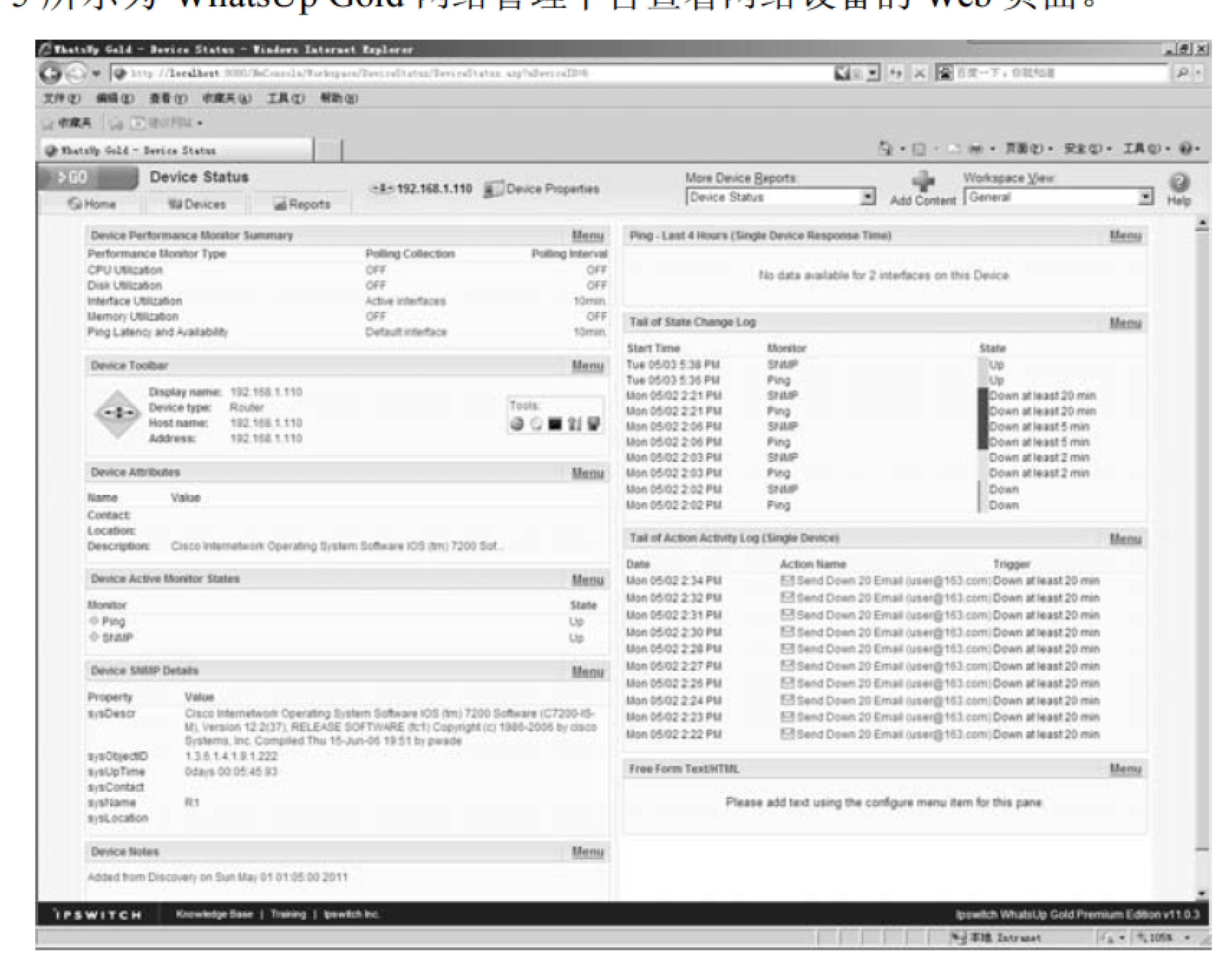


图 5-5

3. HP OpenView

HP OpenView 产品是惠普公司出品的电子业务管理工具程序，被称为“全球 20 大软件公司必备产品”，面向 HP 9000 和 HP e3000 系列服务器的用户群。客户可以利用 OpenView 来管理服务器的应用程序、硬件设备、网络配置和状态，系统性能、业务以及程序维护，还能进行存储管理。HP OpenView 是强大的网络和系统管理工具，是第一个跨平台的网络管理系统。如图 5-6 所示为 HP OpenView 程序的主界面。

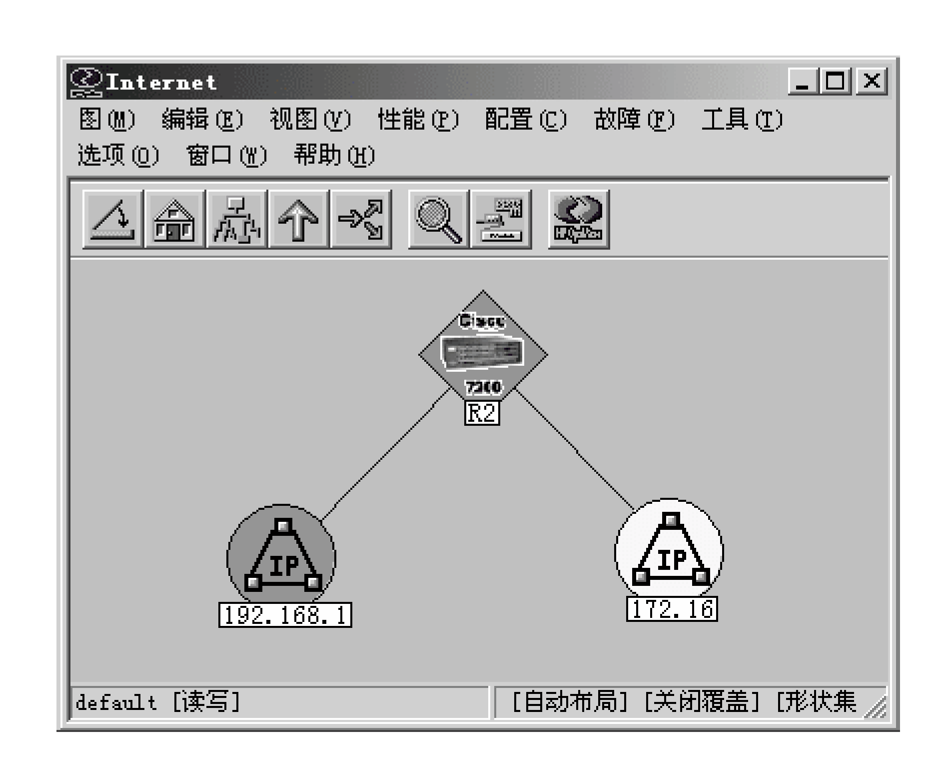


图 5-6

4. IBM Tivoli NetView 网络管理系统

IBM Tivoli 是 IBM IT 服务管理的核心部分。Tivoli 是一个跨越主机系统、客户机/服务器系统、工作组应用、企业网络、Internet 服务器的端到端的解决方案。Tivoli 软件为客户提供了一个无缝集成的、灵活的基础架构管理解决方案，采用强健的安全机制将雇员、业务伙伴和客户连接起来。Tivoli 解决方案主要包括系统管理解决方案，存储管理解决方案和安全管理解决方案。

基于 IBM Tivoli NetView 所提供的网络管理平台，与 Tivoli 的整体管理框架紧密集成，不但能够为用户提供强大的管理能力，而且能够方便地进一步发展到全面的系统管理。

IBM Tivoli 与 Cisco 一直保持着良好的合作关系，NetView 能够与 Ciscoworks2000 紧密集成，实现从 NetView 中调用 CiscoView 以及 Campus Manager 等 Ciscoworks 应用，在 NetView 中显示 Cisco 的图标等等。

如图 5-7 所示为 IBM Tivoli NetView 程序的主界面。

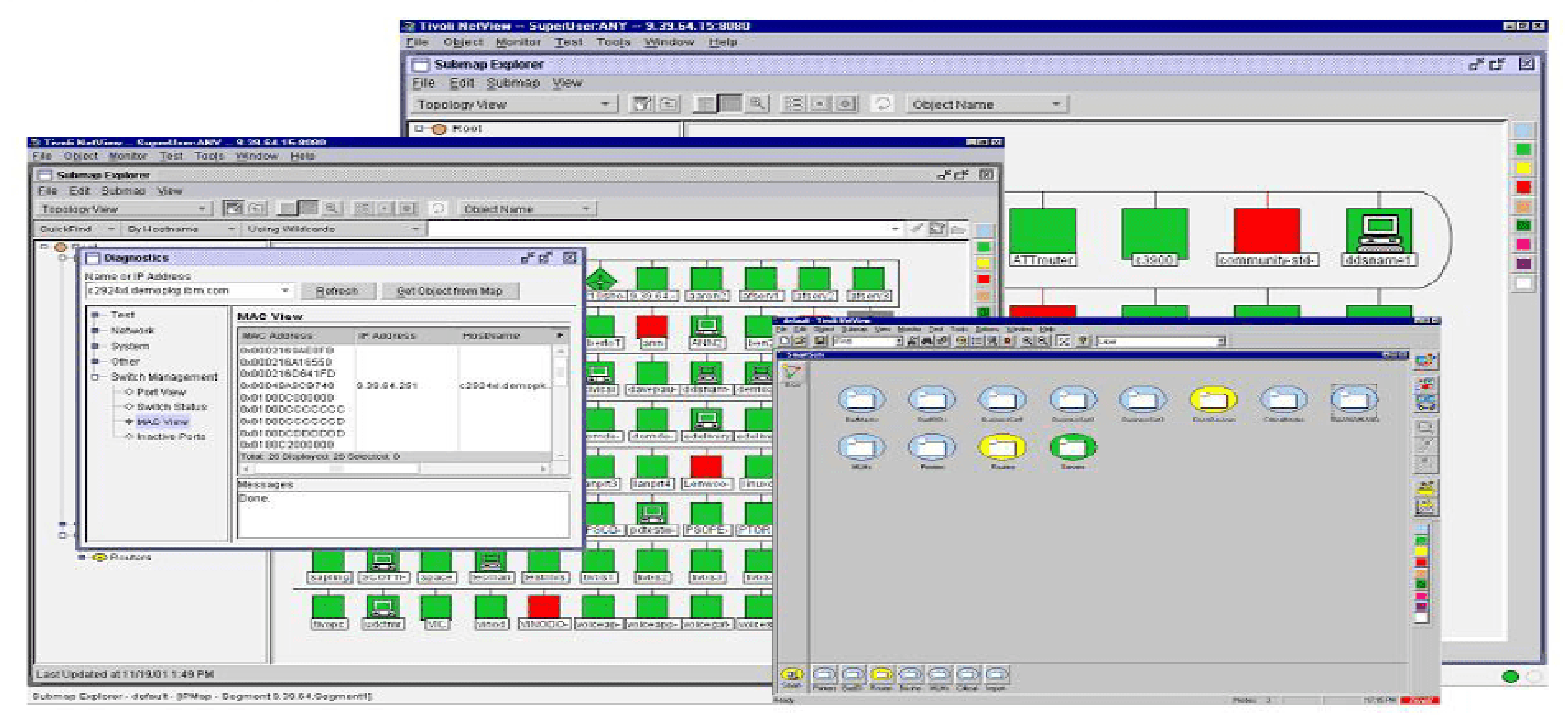


图 5-7

5.2　项目实施 1：搭建 Spiceworks 网络管理平台

搭建网络管理平台，首先需在公司内部所有网络设备上开启 SNMP 管理协议，然后在指定的网络管理设备上安装网络管理平台软件。下面主要介绍 Spiceworks 网络管理平台的搭建及应用方法。

5.2.1　网络管理环境搭建

在安装 Spiceworks 网络管理平台之前，首先要做好基础网络管理环境的搭建。环境搭建的内容主要有以下几方面。

（1）保证目前的网络状态是连通的。

（2）在所有的被管理设备上开启 SNMP 网络管理协议，并设置团体名为【public】。

（3）网络管理设备的机器性能要相对稳定，一般要选择 Windows Server 2003/2008 服务器。

（4）网络管理操作界面以网页形式实现，IE 浏览器要支持 JavaScript、CSS 动态网页的浏览。

5.2.2　架设网络管理平台

网络管理环境搭建完成后，下面就可以架设网络管理平台。在 Windows Server 2003 服务器中架设 Spiceworks 网络管理平台的具体方法如下。

1. 安装 Spiceworks

安装 Spiceworks 的具体步骤如下。

01 运行安装程序进入安装界面。在【spiceworks will run on port number】（spiceworks 将要使用的默认端口）文本框中输入连接管理网页所使用的端口，默认值为“80”，单击【Next】（下一步）按钮，如图 5-8 所示。

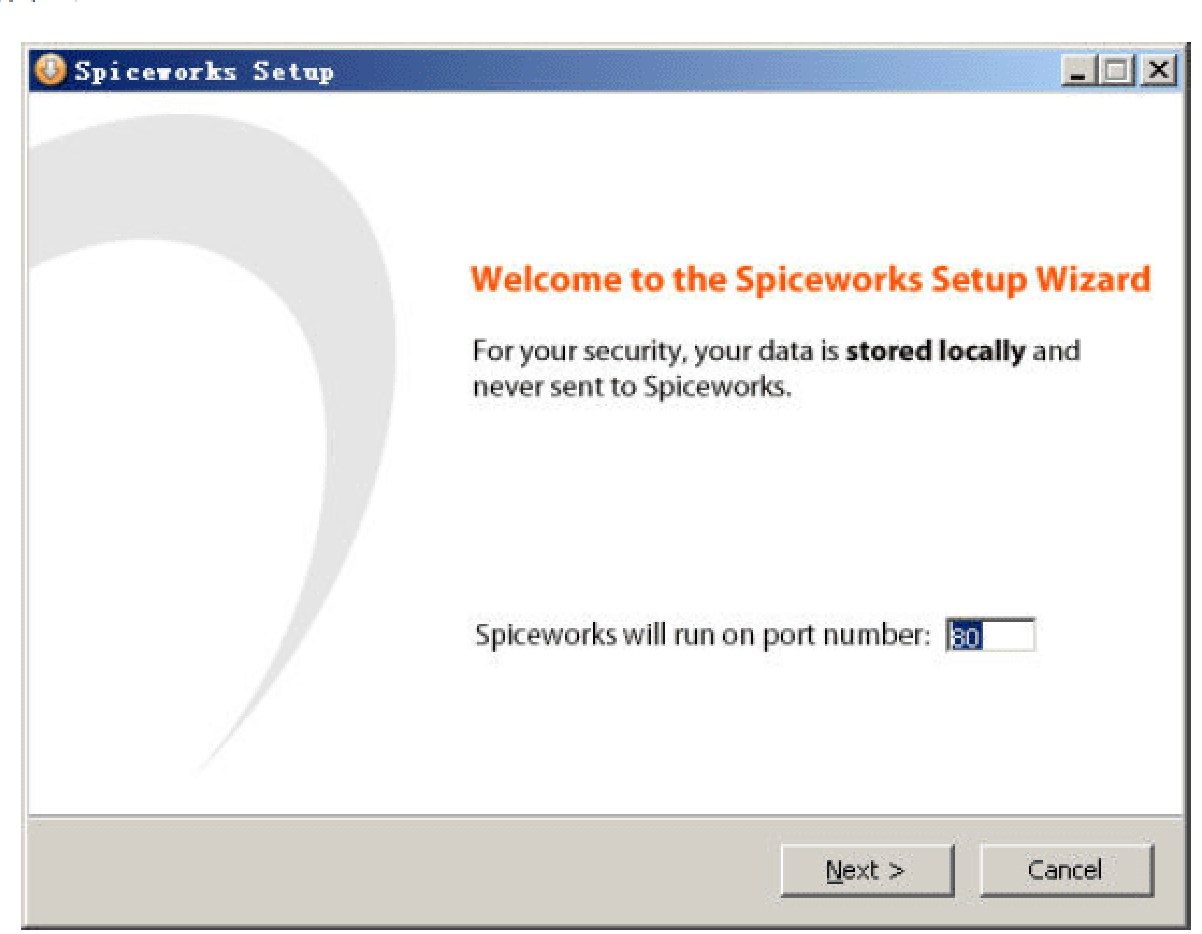


图 5-8

02 在弹出的对话框中选择【I accept these terms of use and Privacy policy】（我接受使用条款

和政策）复选框，接受许可协议，单击【Next】（下一步）按钮，如图 5-9 所示。

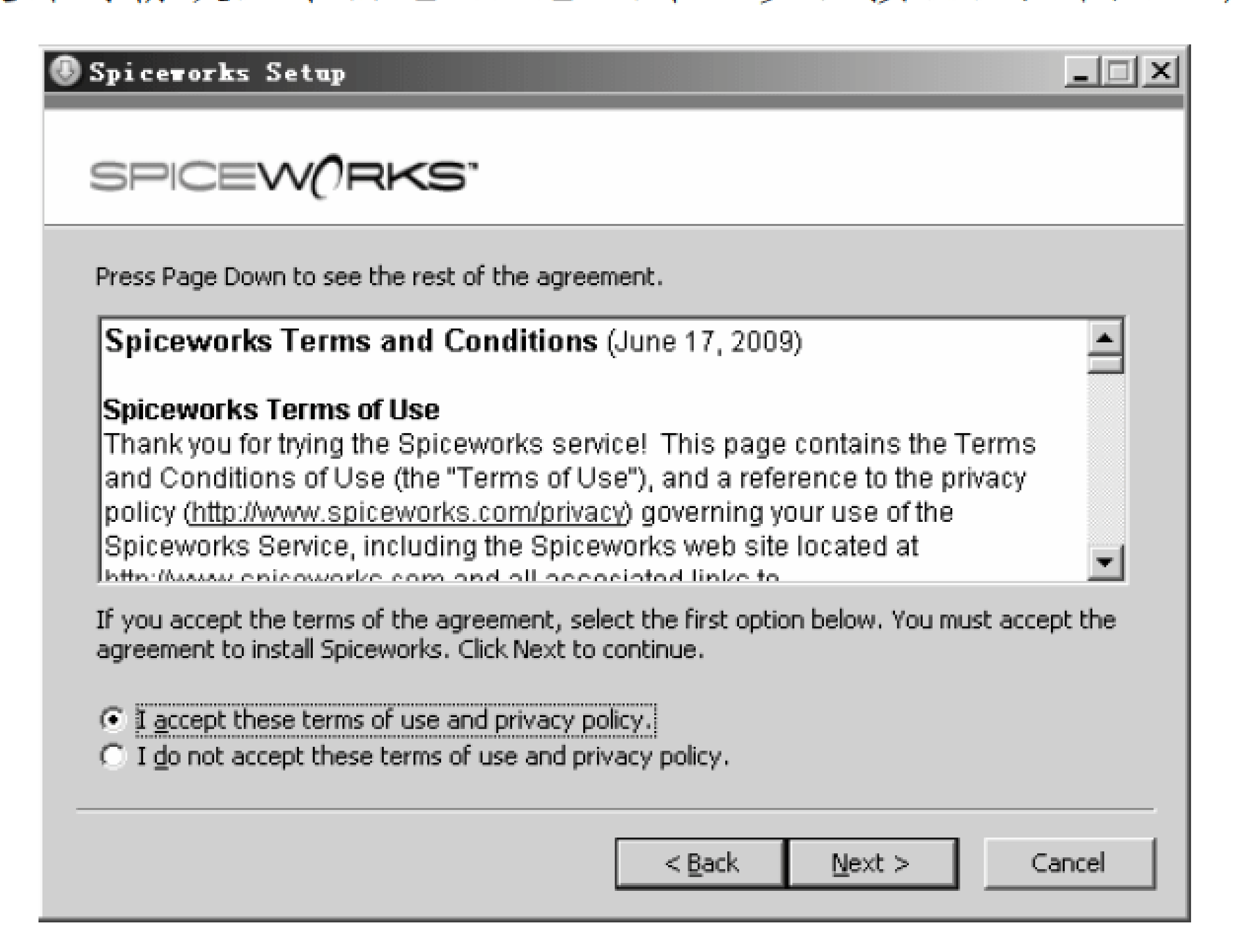


图 5-9

03 在弹出的对话框中单击【Browse】(浏览)按钮，可以选择安装路径。本实例选择默认的安装路径，单击【Install】（安装）按钮，如图 5-10 所示。

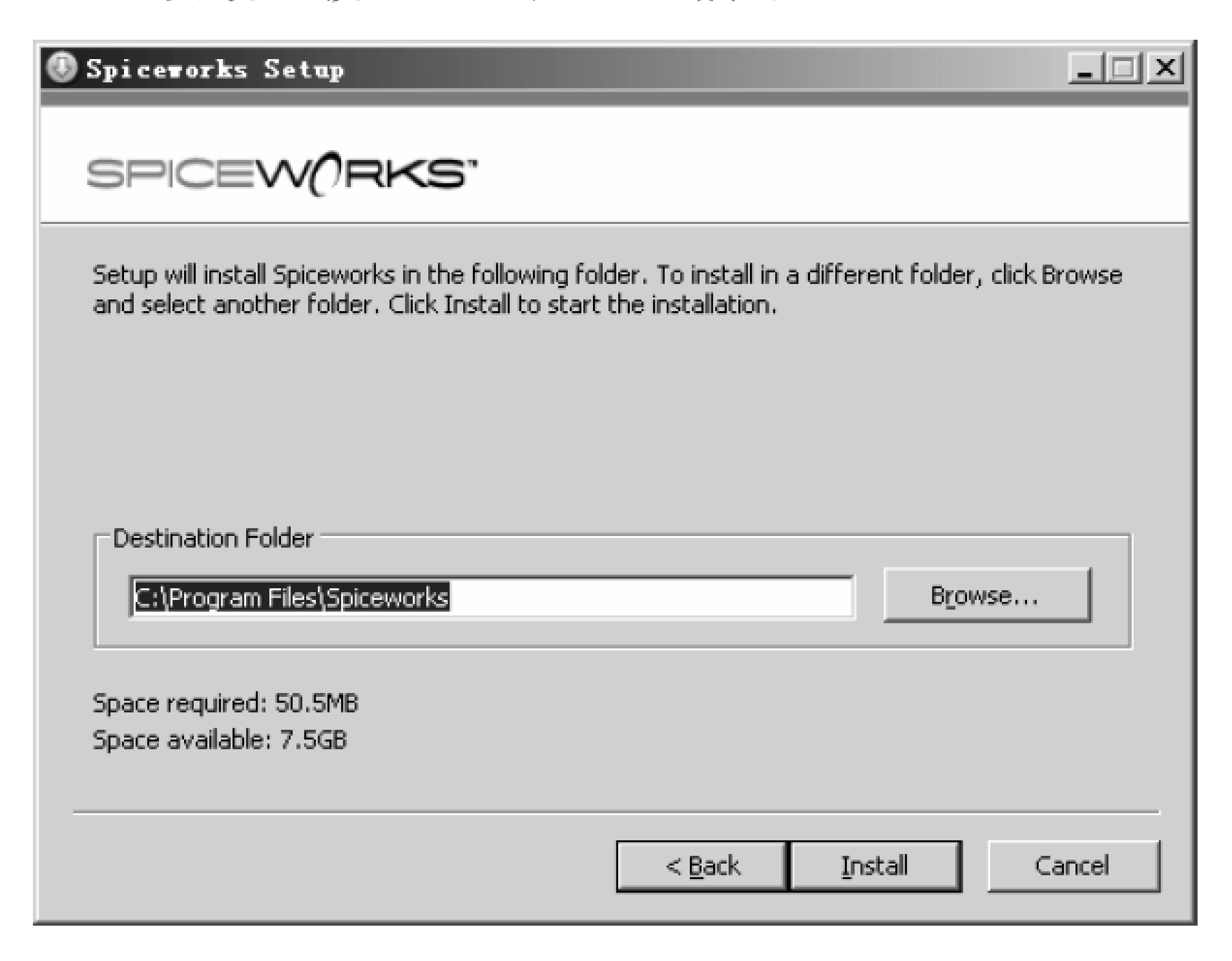


图 5-10

04 系统开始自动安装 Spiceworks，并显示安装的进度，如图 5-11 所示。

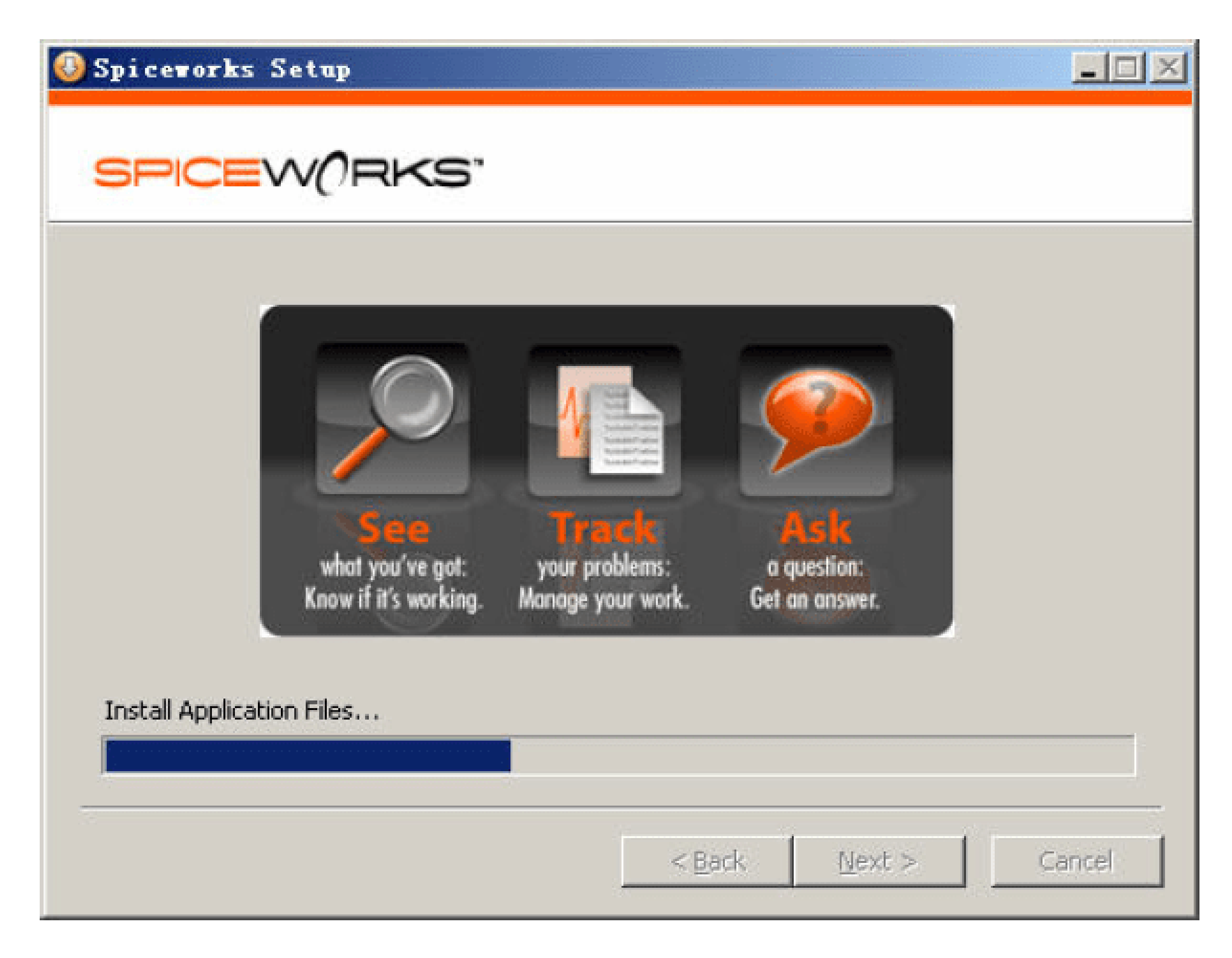


图 5-11

05 安装完成后，在弹出的对话框中选择【Install Desktop Shortcut】（创建桌面快捷方式）和【Run Spiceworks Now】（马上运行 Spiceworks）复选框，单击【Finish】（完成）按钮，如图 5-12 所示。

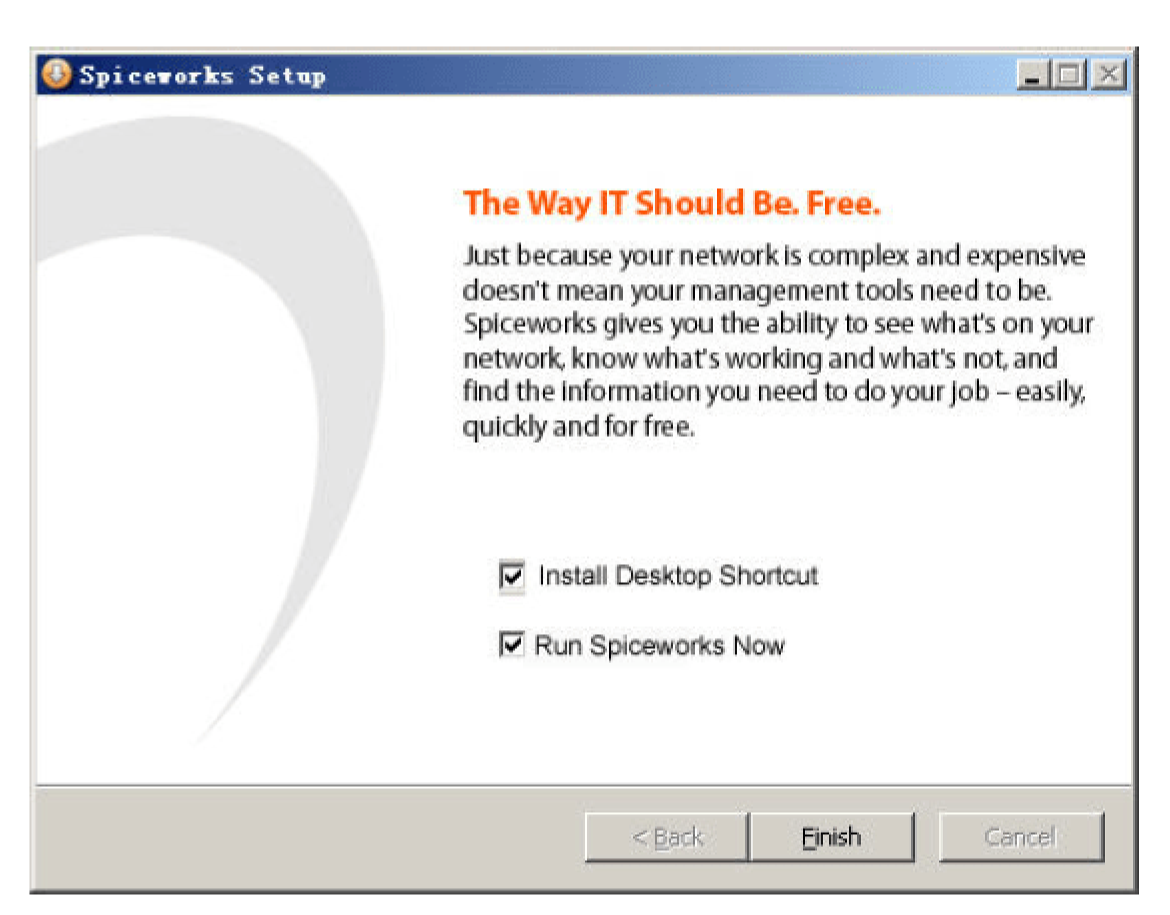


图 5-12

06 系统自动启动 Spiceworks 网络管理平台，并显示加载的进度，如图 5-13 所示。

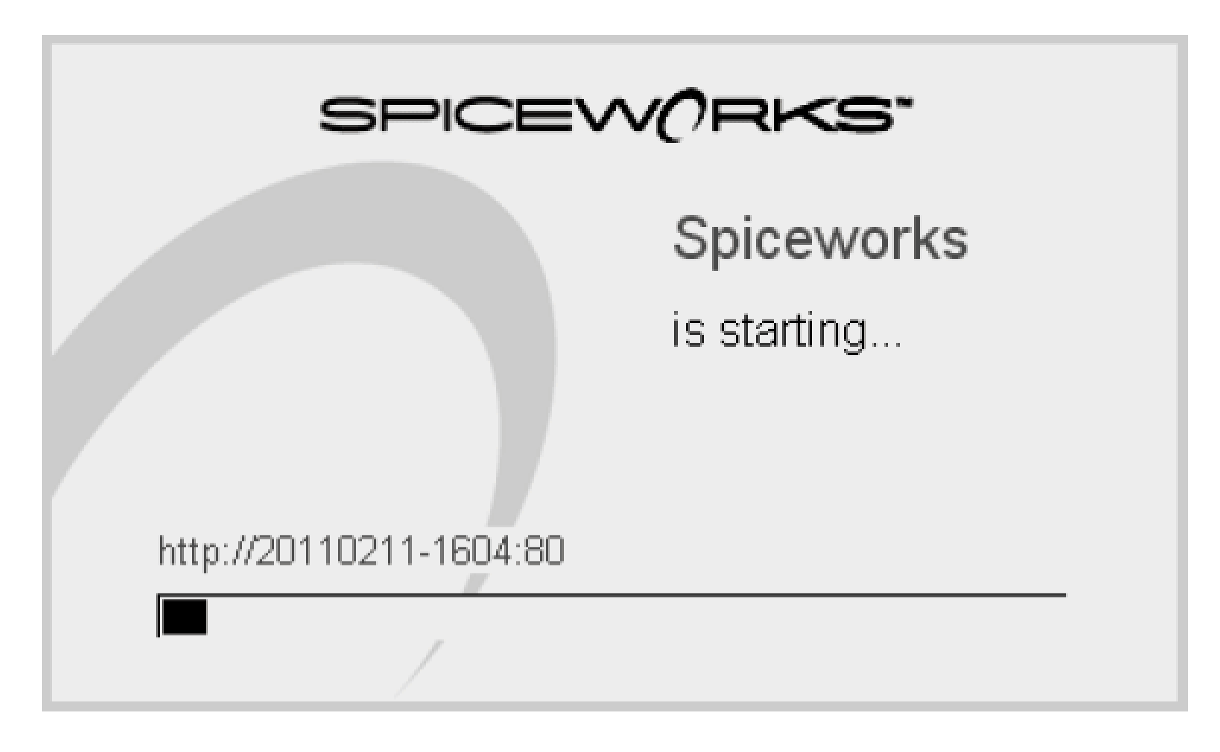


图 5-13

07 加载完成后，登录到 Spiceworks 网络管理平台后自动弹出用户信息录入网页，在页面中分别输入相应的信息，单击【Next】（下一步）按钮，Spiceworks 网络管理平台的安装已经完成，如图 5-14 所示。

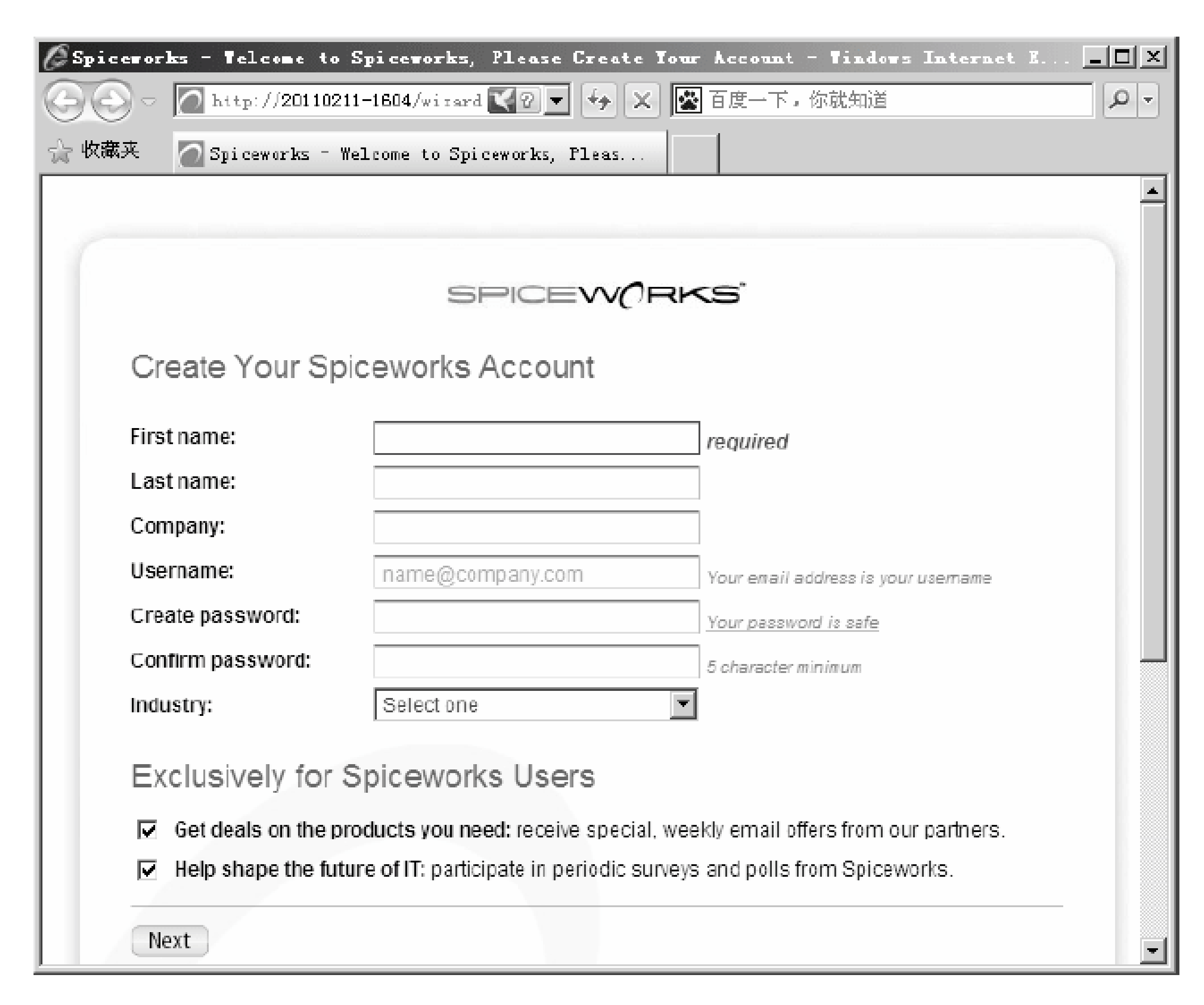


图 5-14

图 5-14 所示的页面中各个字段的含义如下。

（1）【First name】（名字）：录入用户名字。

（2）【Last name】（姓氏）：录入用户姓氏。

（3）【Commpany】（公司）：录入所在公司。

（4）【Username】（用户名）：设定登录 Spiceworks 网络管理平台的用户名，格式为邮箱地址，此地址尽量为可用地址。

（5）【Create password】（输入密码）：设定登录密码。

（6）【Confirm password】（重新输入密码）：确认密码。

（7）【Industry】（行业）：选择应用行业。

2. 网络扫描

刚安装好的 Spiceworks 网络管理平台没有任何网络环境信息，需要进行网络扫描获得网络环境信息。第一次使用 Spiceworks 网络管理平台进行网络扫描的具体操作步骤如下。

01 用户信息设置完成后，进入 Spiceworks 环境页面，单击【Start with Inventory】（以清单形式开启）选项，如图 5-15 所示。

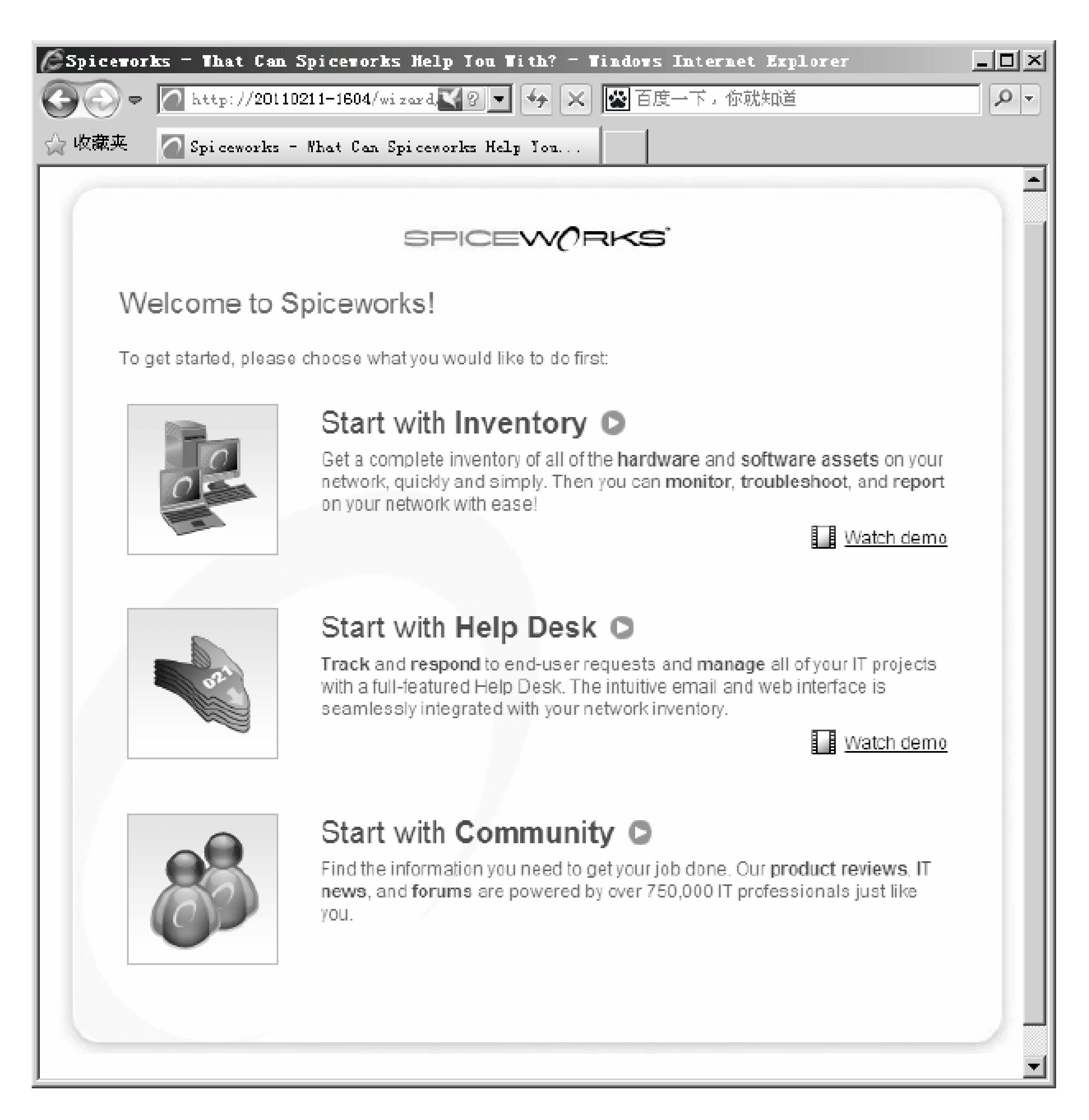


图 5-15

02 第一次进入管理页面，没有设备信息清单，会弹出【What would you like to Lnventory】（如何获得清单）页面，单击【Scan my entire network】（扫描全部网络）超级链接，如图 5-16 所示。



图 5-16

03 弹出【Scan Settings】（扫描设置）页面。根据网络的实际情况选择不同的系统。如果本地主机都是使用 Windows 系统，设置如图 5-17 所示，单击【Next】（下一步）按钮。

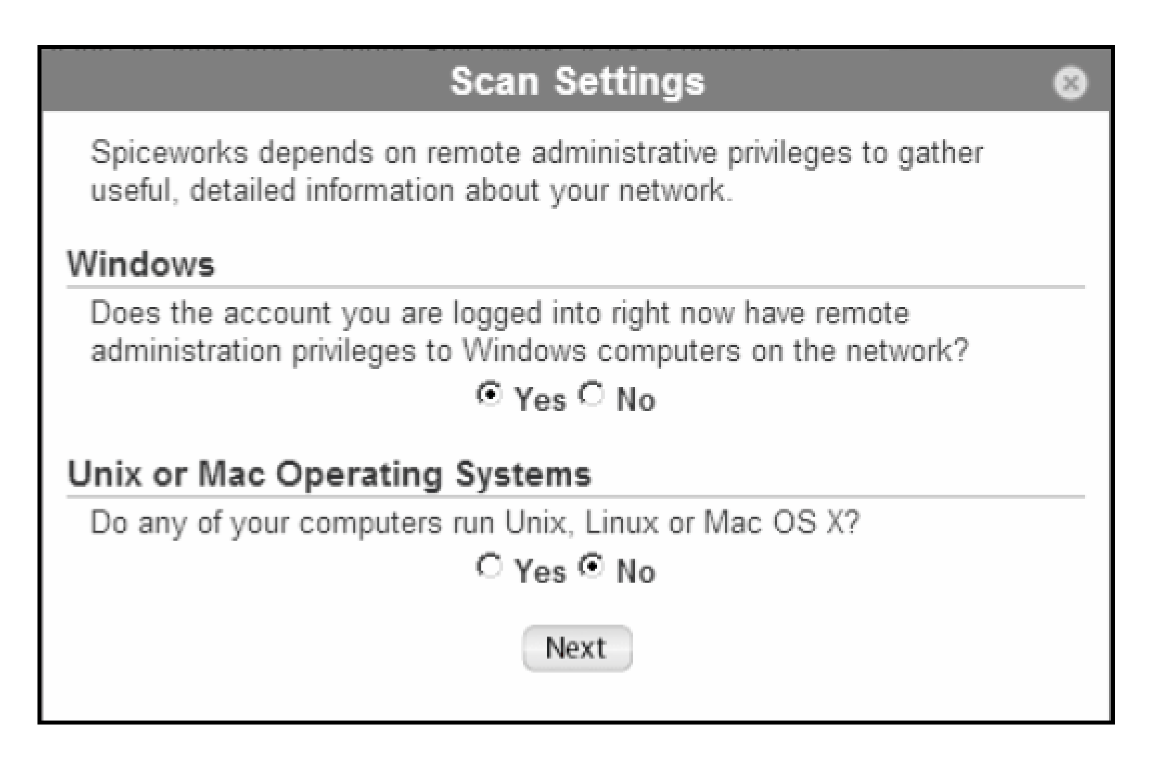


图 5-17

04 如果本地主机有 Unix/Linux 等系统，设置如图 5-18 所示，并在【Username】（用户名）和【Password】（密码）文本框中输入使用 SSH 连接该系统使用的用户名及密码，单击【Next】（下一步）按钮。

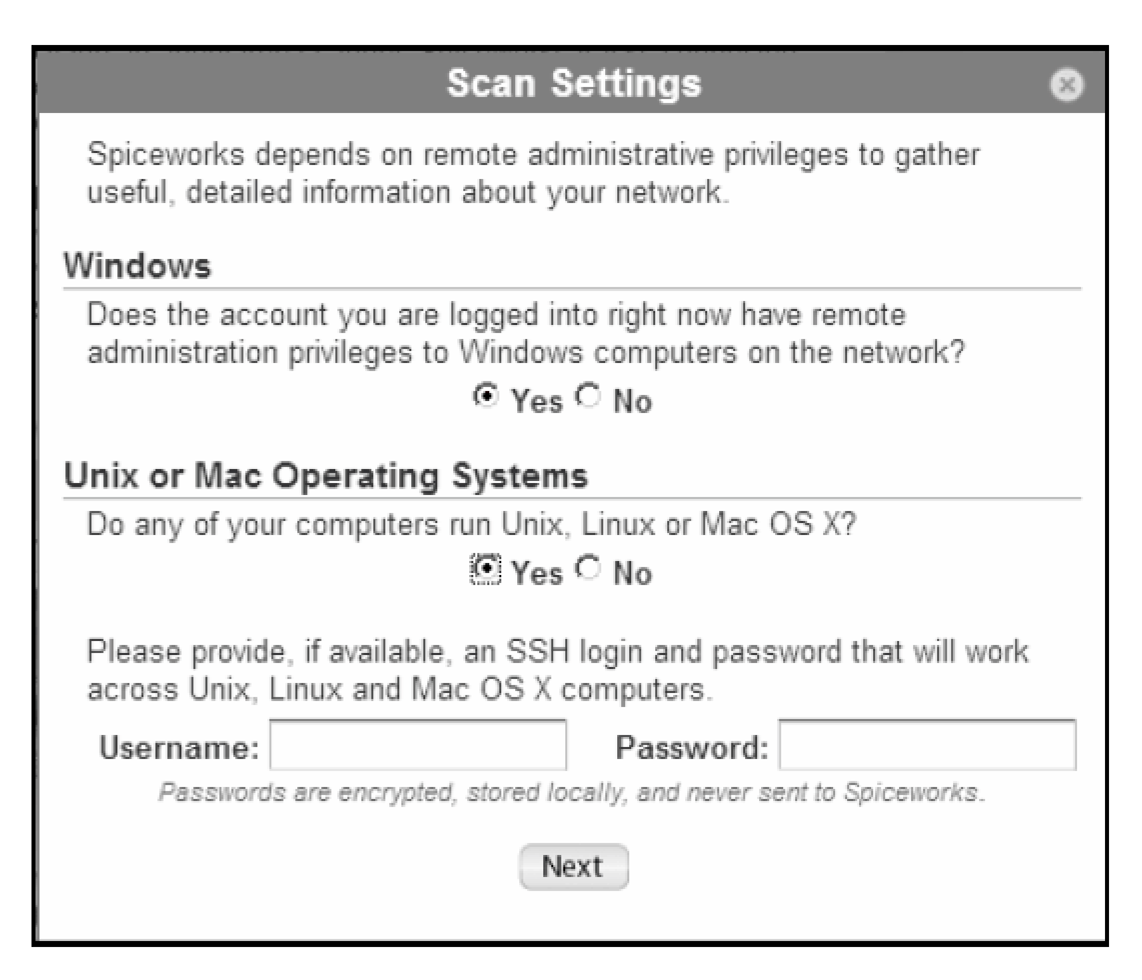


图 5-18

05 弹出【Getting ready to inventory your network】（准备库存网络）页面，默认对该服务器所在网段“192.168.1.1-254”范围内的所有设备进行扫描，单击【Start】（开始）按钮，如图 5-19 所示。

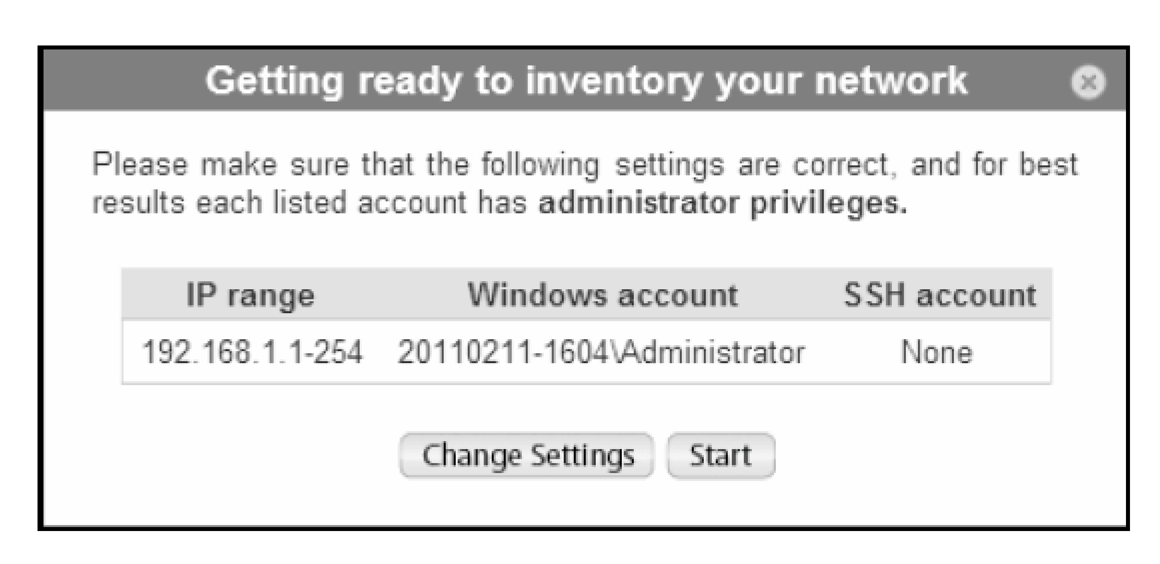


图 5-19

06 弹出【Spiceworks Updates】（Spiceworks 更新提示）页面，单击【OK】（确定）按钮，如图 5-20 所示。

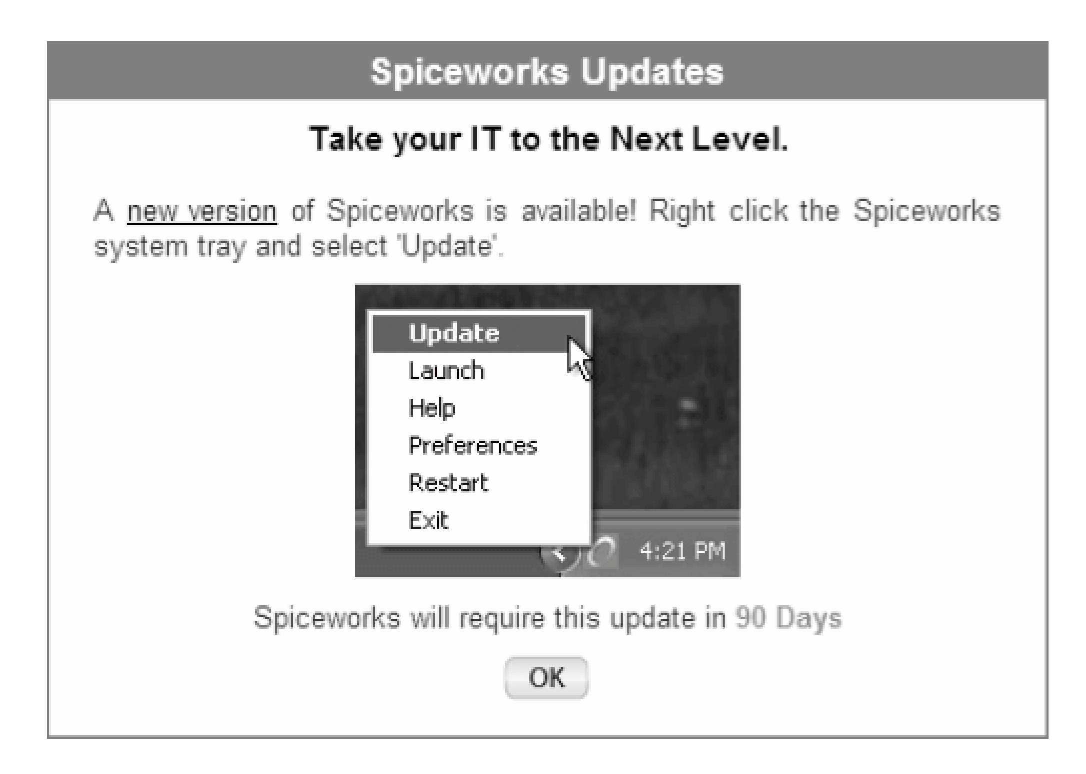


图 5-20

07 系统进入扫描页面，自动对“192.168.1.1-254”网段的所有设备进行扫描，如图 5-21 所示。

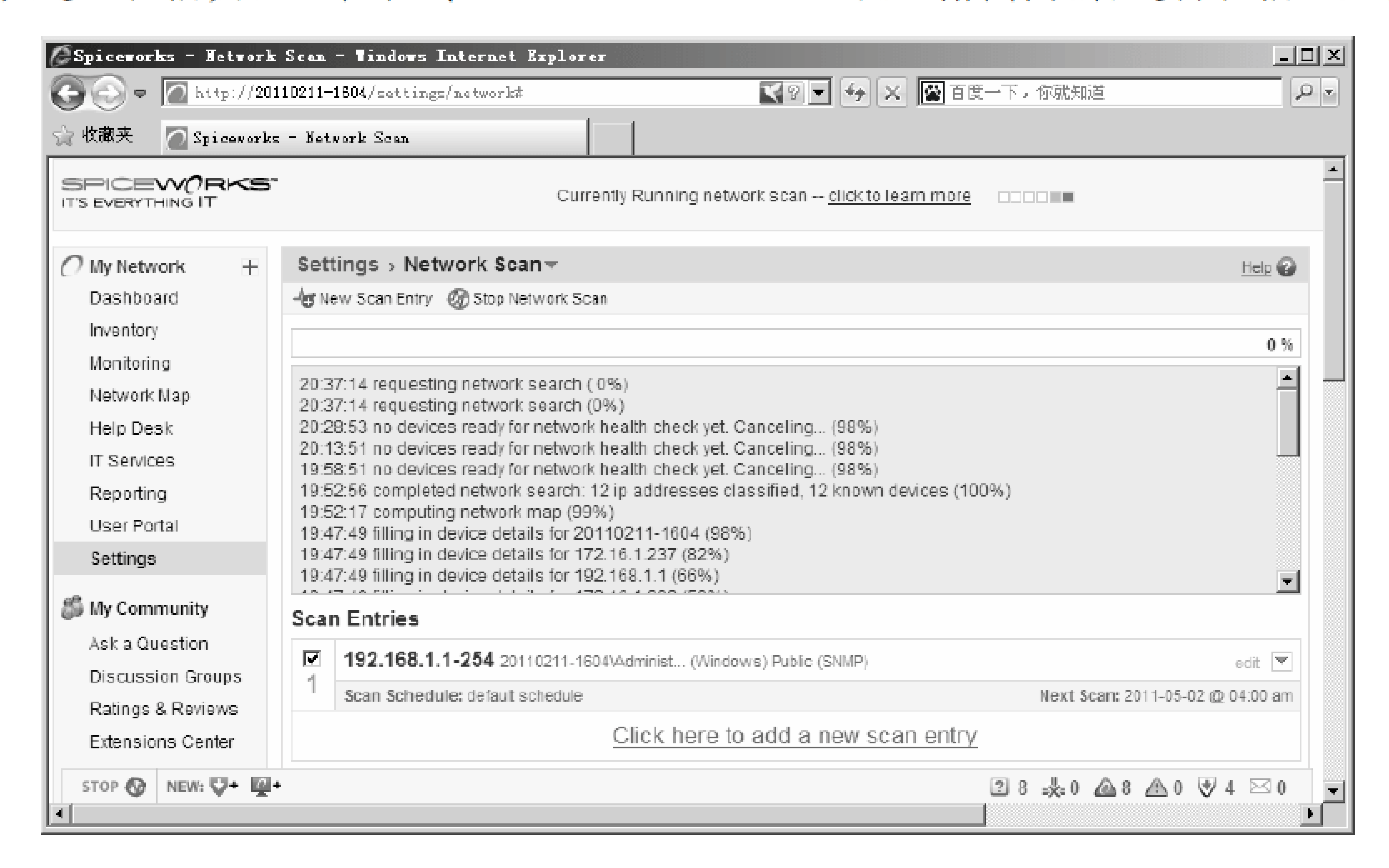


图 5-21

3. 扫描指定网段的网络拓扑结构

默认情况下，Spiceworks 只对服务器所在网段的设备扫描，如果需要扫描其他网段，必须手工设置。

本实例以扫描范围“172.16.1.1-254”为例讲述如何手动设置，具体操作步骤如下。

01 在【Getting ready to inventory your network】（准备库存网络）页面中，单击【Change Settings】（改变设置）按钮，如图 5-22 所示。

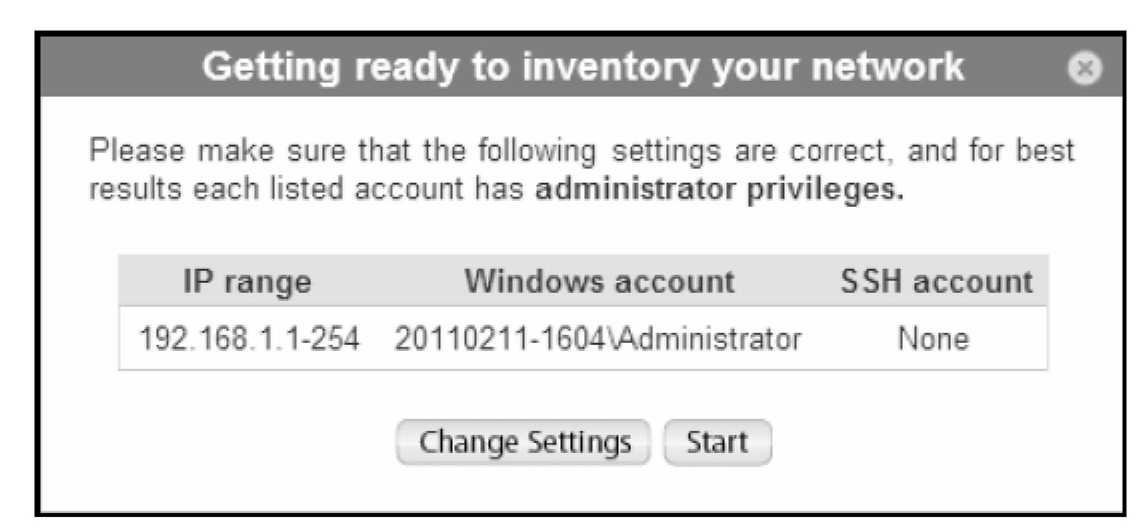


图 5-22

02 进入扫描网络设置页面，单击【Click here to add a new scan entry】（单击这里添加新扫描网络）超级链接，如图 5-23 所示。

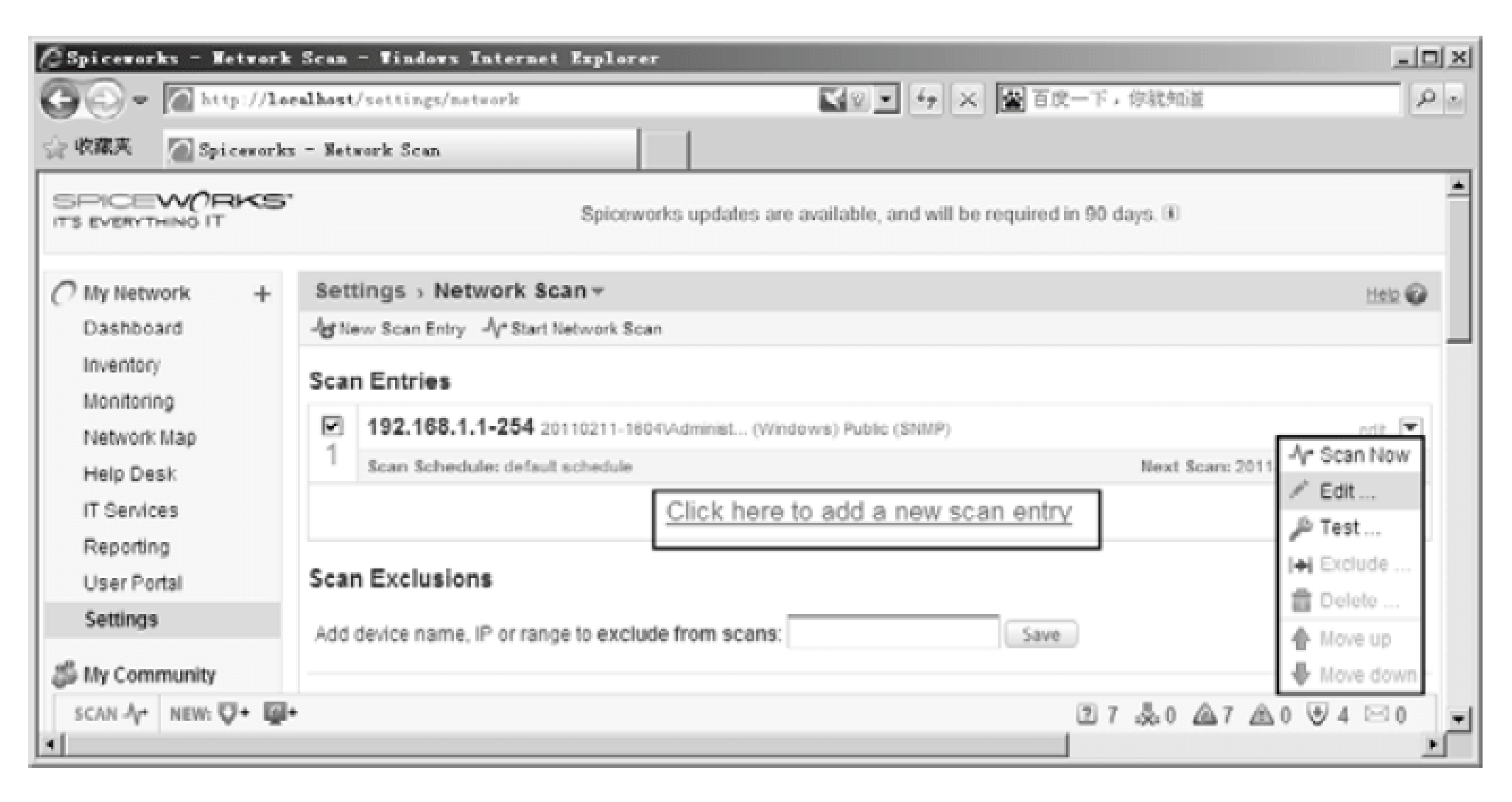


图 5-23

03 弹出【Add New Scan Entry】（添加新扫描网络）页面，在【Device/Range】（设备或组）文本框中输入扫描范围“172.16.1.1-254”，该文本框还可输入区域名，如图 5-24 所示。

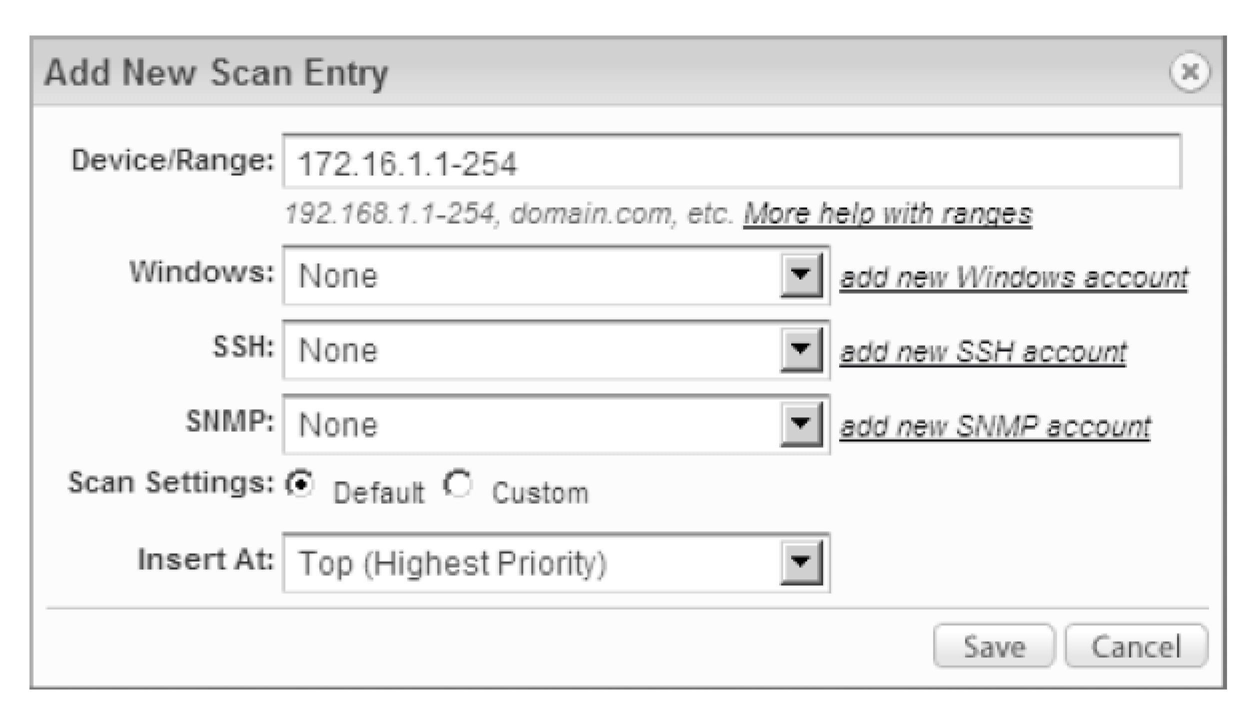


图 5-24

04 在【SNMP】（简单网络管理协议）文本框中选择“Public”为 SNMP 协议的团体名（也可根据实际情况单击【add new SNMP account】（添加新 SNMP 清单）超级链接，添加新的团体名），单击【Save】（保存）按钮，如图 5-25 所示。

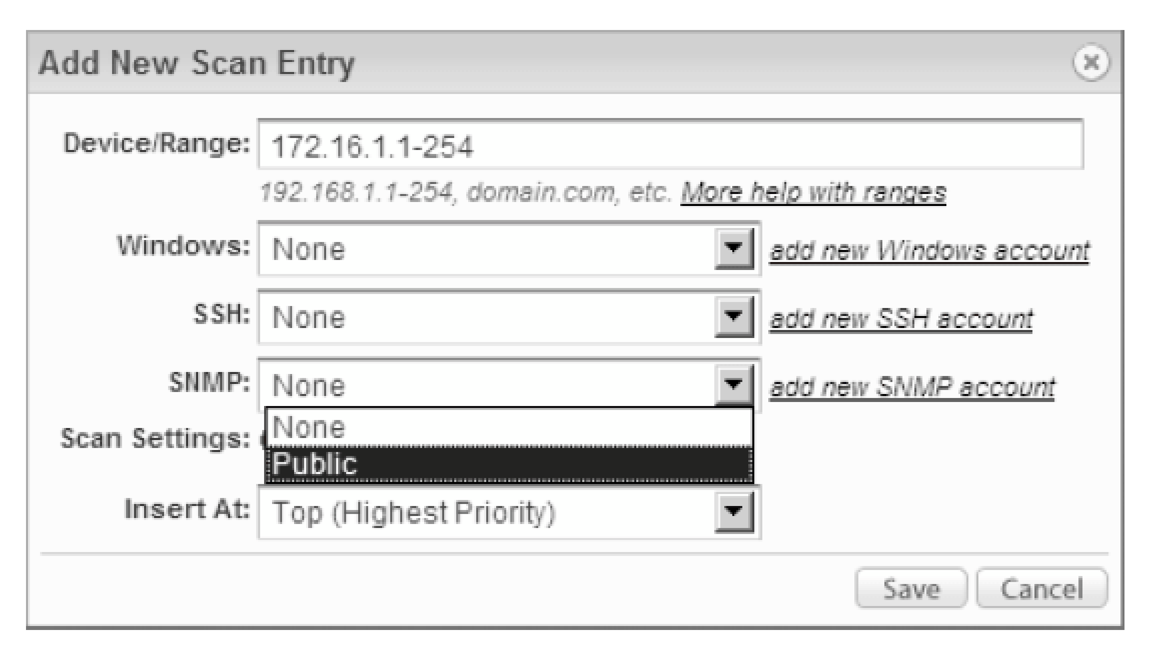


图 5-25

05 新扫描范围添加成功，选择全部扫描范围，单击【Start Network Scan】（开始网络扫描）

超级链接，如图 5-26 所示。

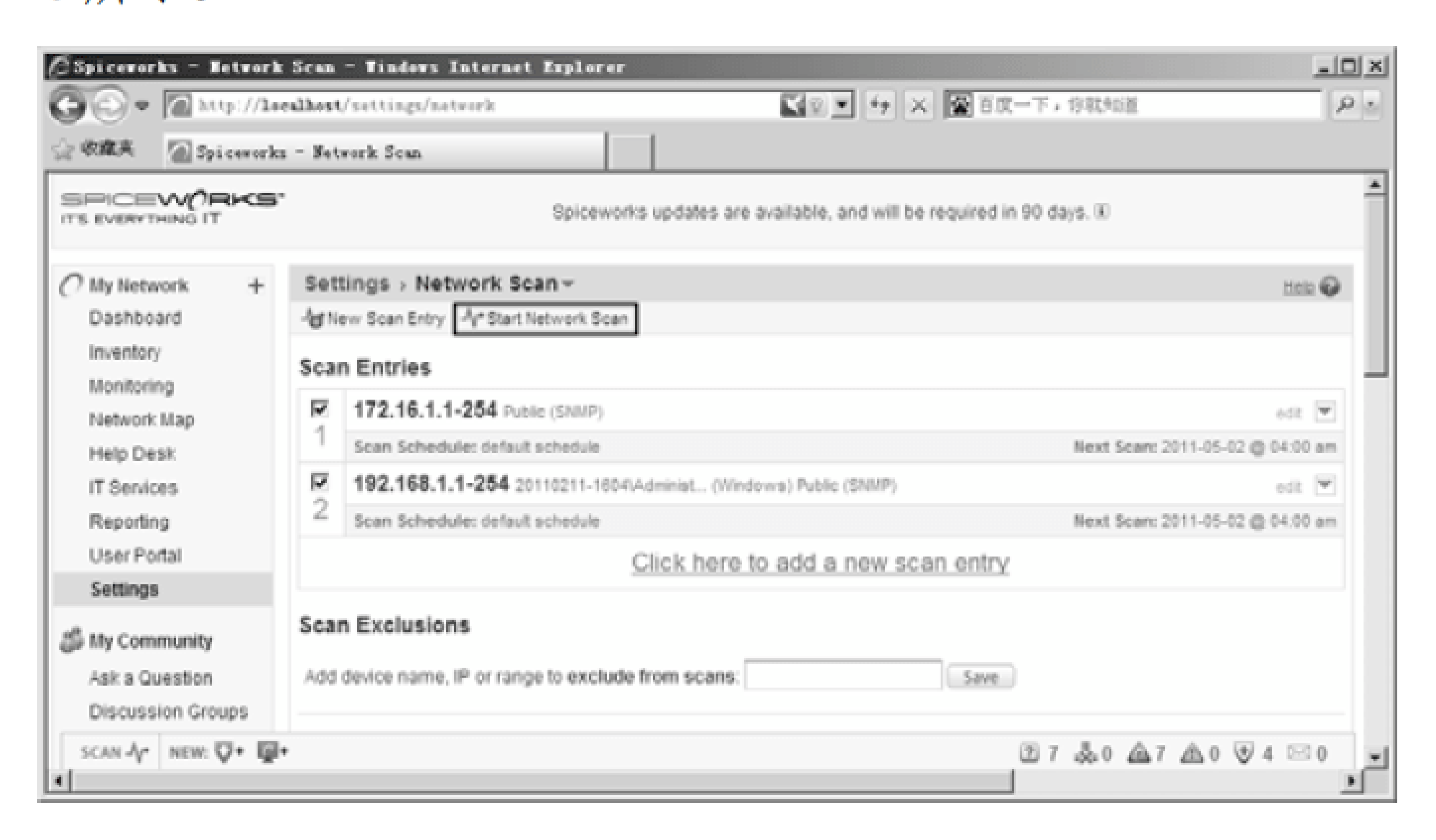


图 5-26

06 弹出【Getting ready to inventory your network】（准备库存网络）页面，单击【Start】（开始）按钮即可开始扫描自定义的网络，如图 5-27 所示。

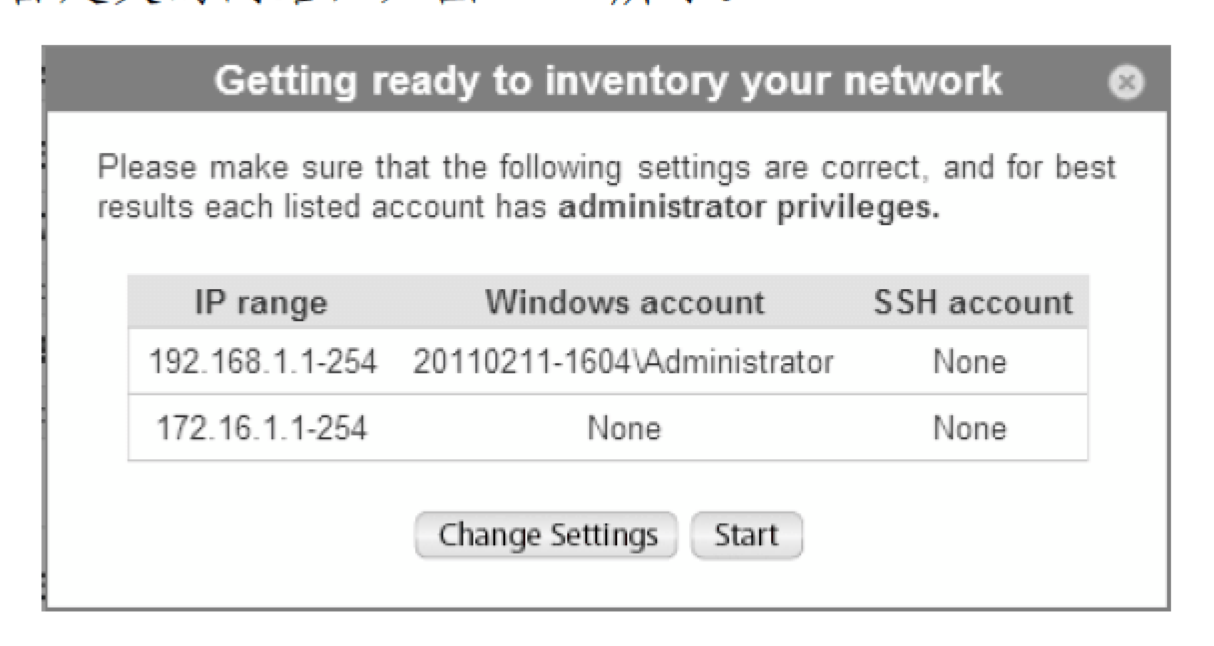


图 5-27

4. 通过 Network Map 模块查看网络拓扑及信息

网络扫描结束后，需要清晰直观地查看网络信息，可以使用 Spiceworks 网络管理平台提供的 Network Map 模块。

使用 Network Map 模块的具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择【Network Map】（网络地图）选项，在页面右侧窗格中显示出扫描后的网络拓扑图，拓扑图中每一个图标代表一个设备。可以通过，如图 5-27 所示，如图 5-27 所示图形缩放、移动工具调整拓扑图大小及位置，也可以通过鼠标单击拖曳或滑轮改变拓扑布局及大小，如图 5-28 所示。

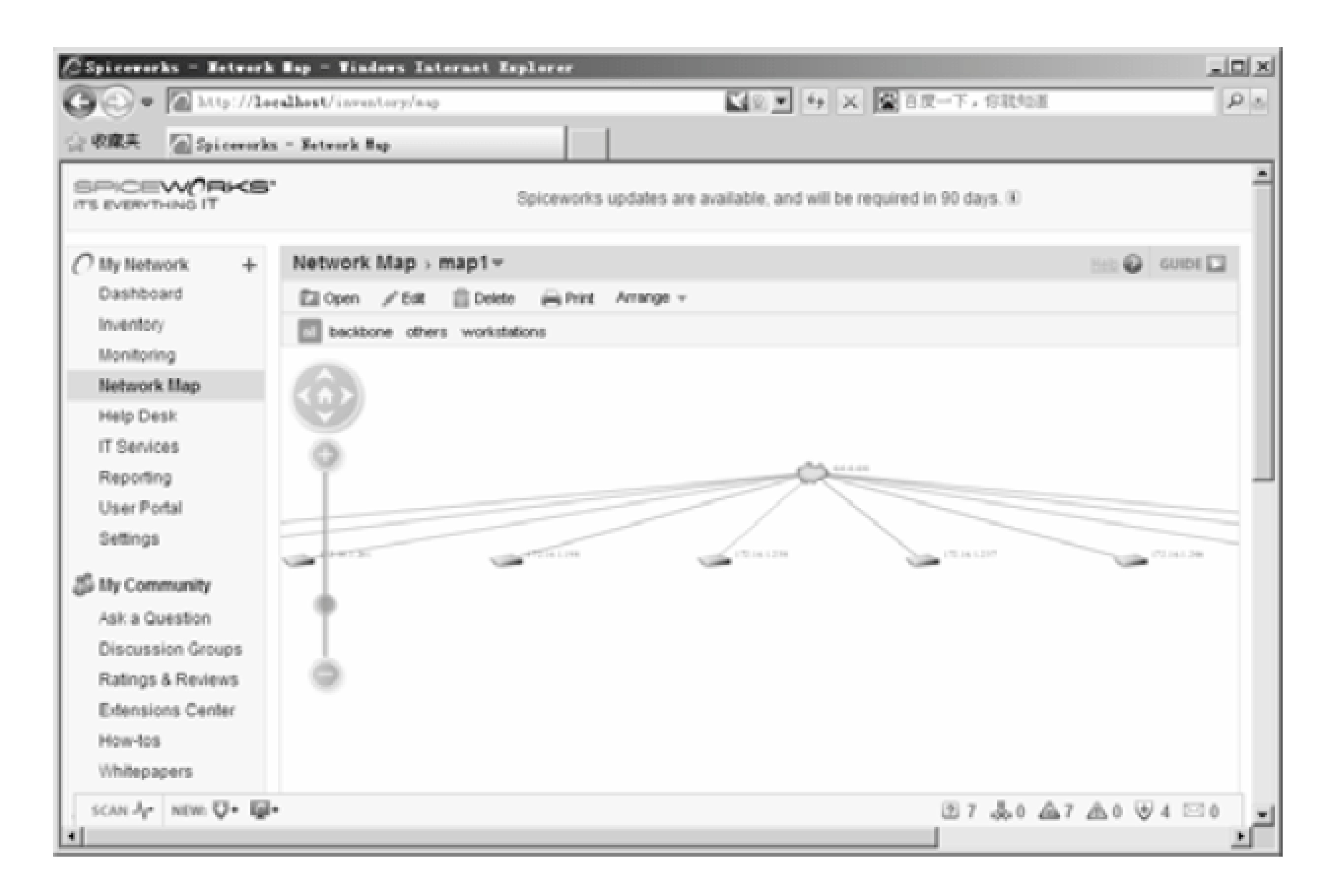


图 5-28

02 软件默认为【Hierarchy Layout】（分层布局）模式。选择【Arrange】（布局）➢【Radial Layout】（放射状）菜单命令，改变网络拓扑图显示方式，如图 5-29 所示。

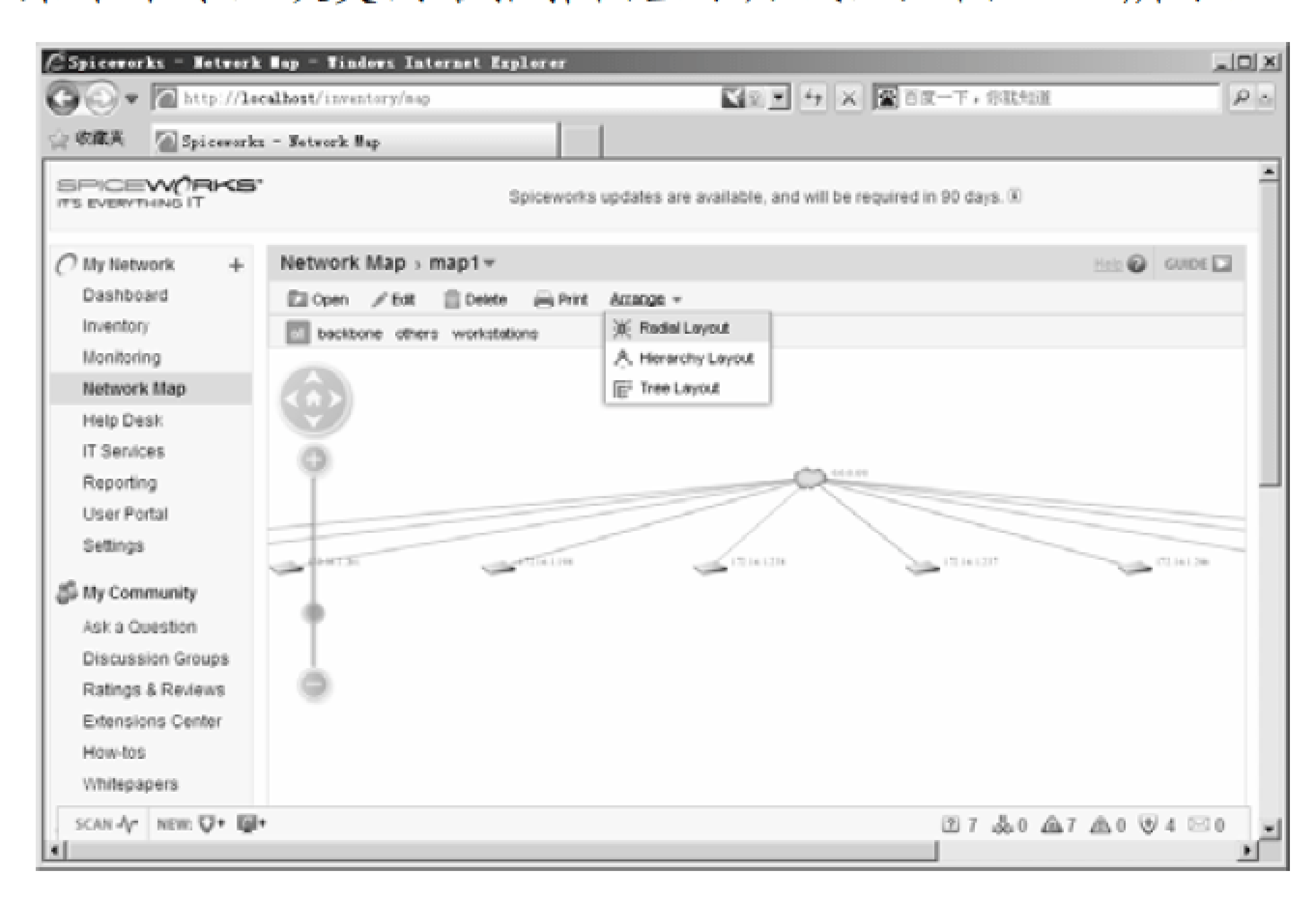


图 5-29

03 改变后的拓扑图模式如图 5-30 所示，表现为放射状。

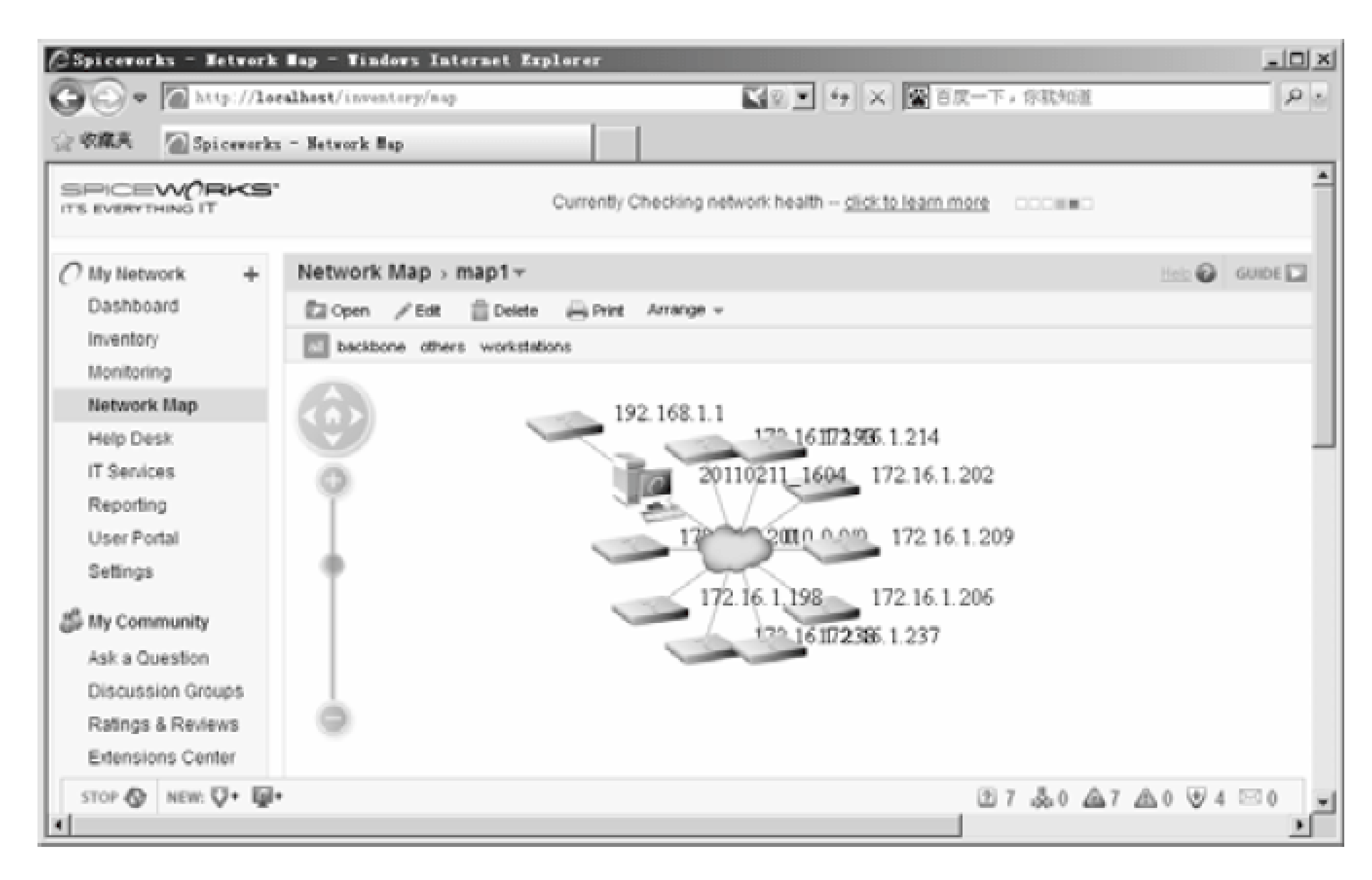


图 5-30

04 单击网络设备的图标并拖曳到适当的位置，将网络拓扑图调整得更加直观，如图 5-31 所示。

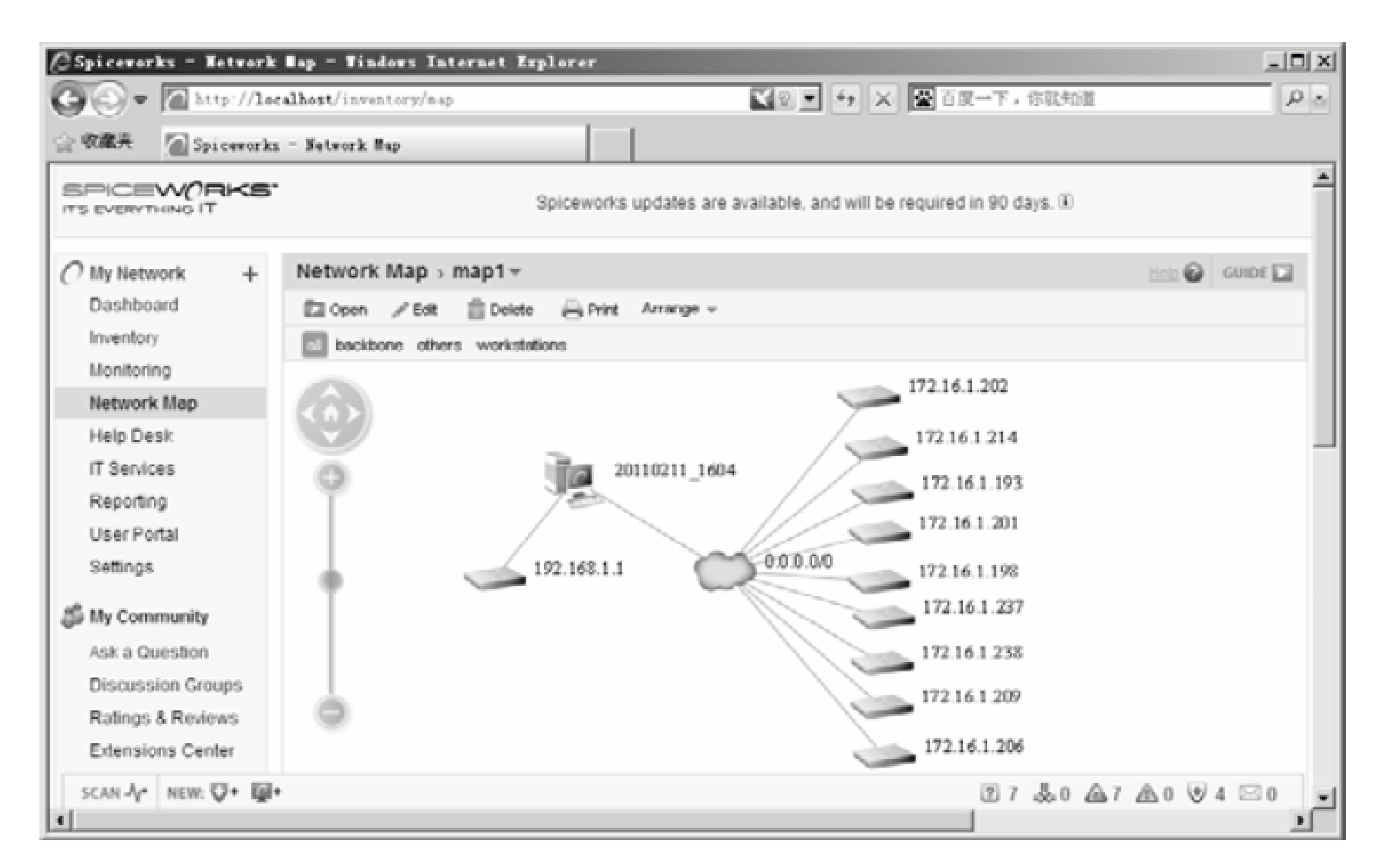


图 5-31

05 单击想要查看的设备图标，弹出该设备的摘要信息框，如图 5-32 所示。

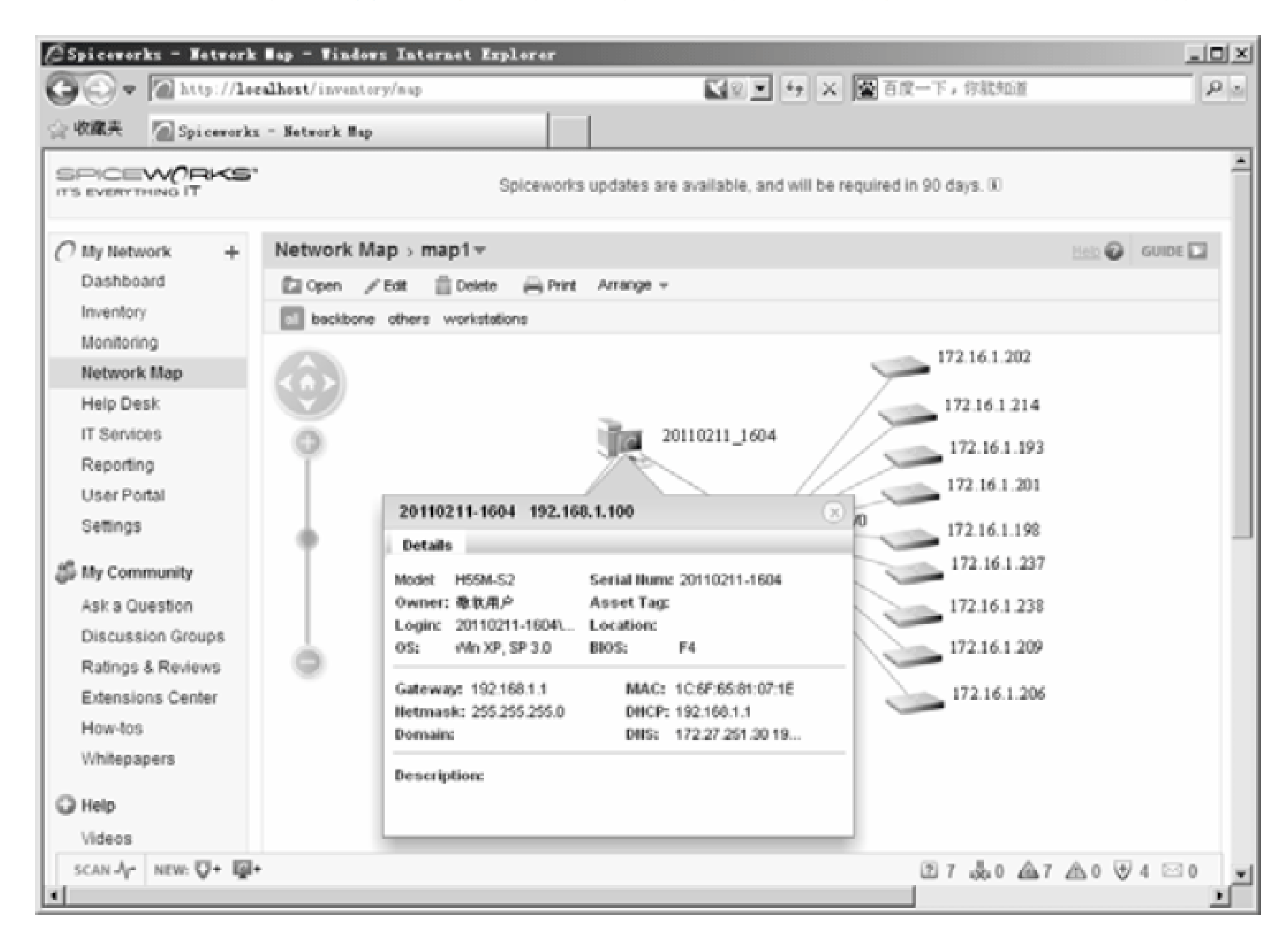


图 5-32

06 单击【Edit】（编辑）超级链接，打开网络拓扑图编辑页面，在该页面也可以调整网络拓扑图，调整完成之后，单击【Save】（保存）按钮，如图 5-33 所示。

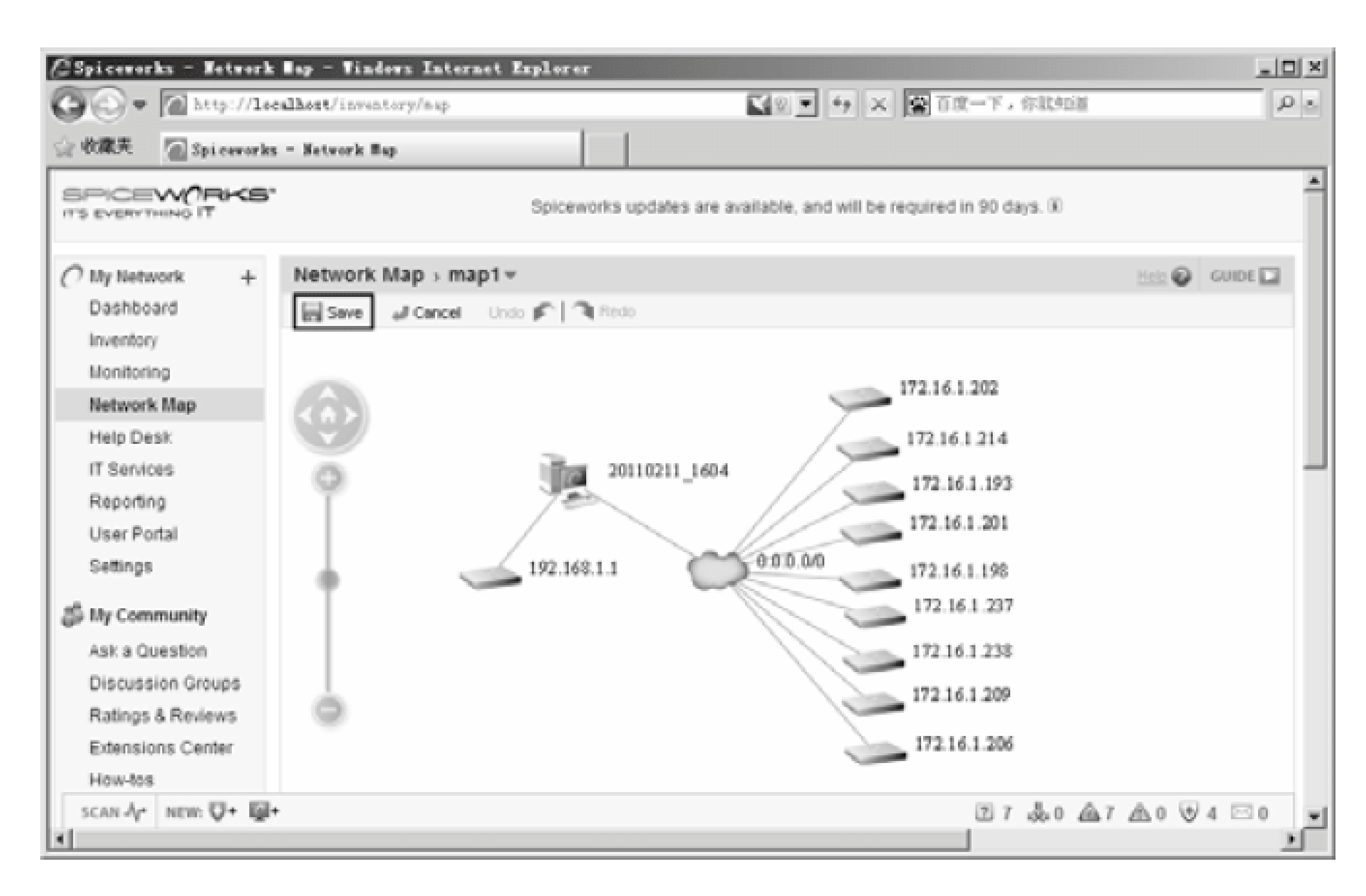


图 5-33

07 弹出【Save the map】（保存地图）页面，单击【Save new】（保存新名）按钮，如图 5-34 所示。

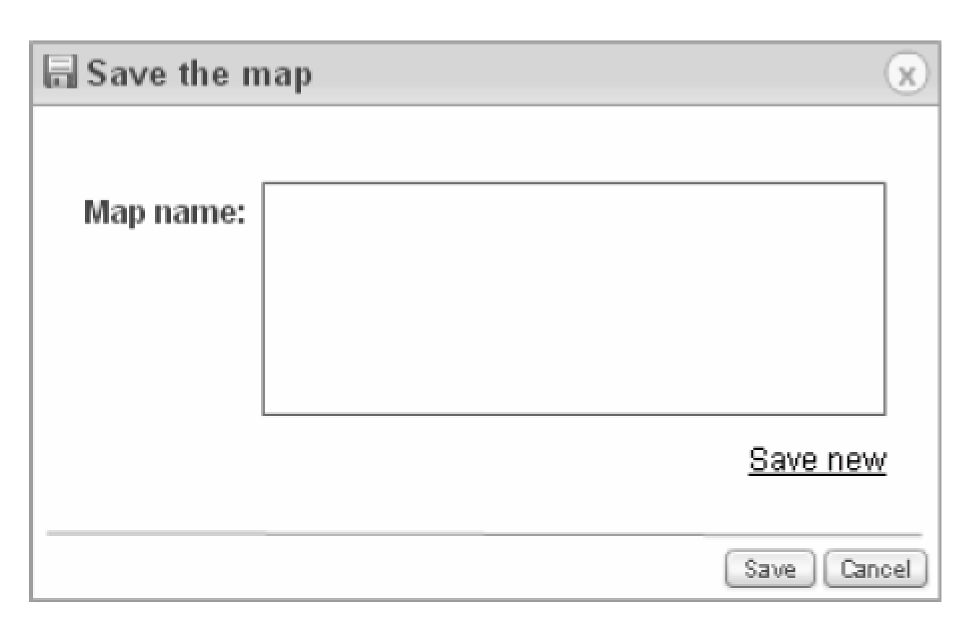


图 5-34

08 在【Map name】（地图名字）文本框中输入网络拓扑图的名字（可用时间、范围等信息作为网络拓扑图名字，以方便记忆、查询），单击【Save】（保存）按钮，如图 5-35 所示。

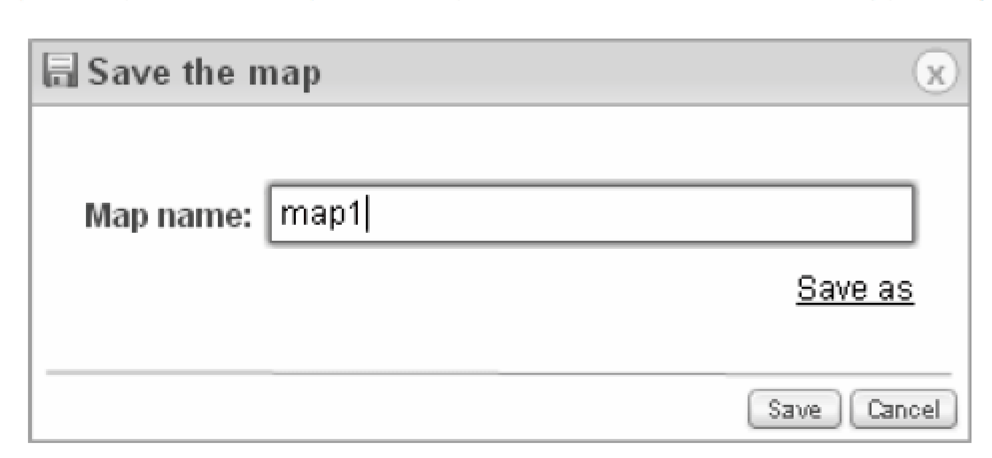


图 5-35

09 返回到软件主界面，单击【Open】（打开）按钮，如图 5-36 所示。

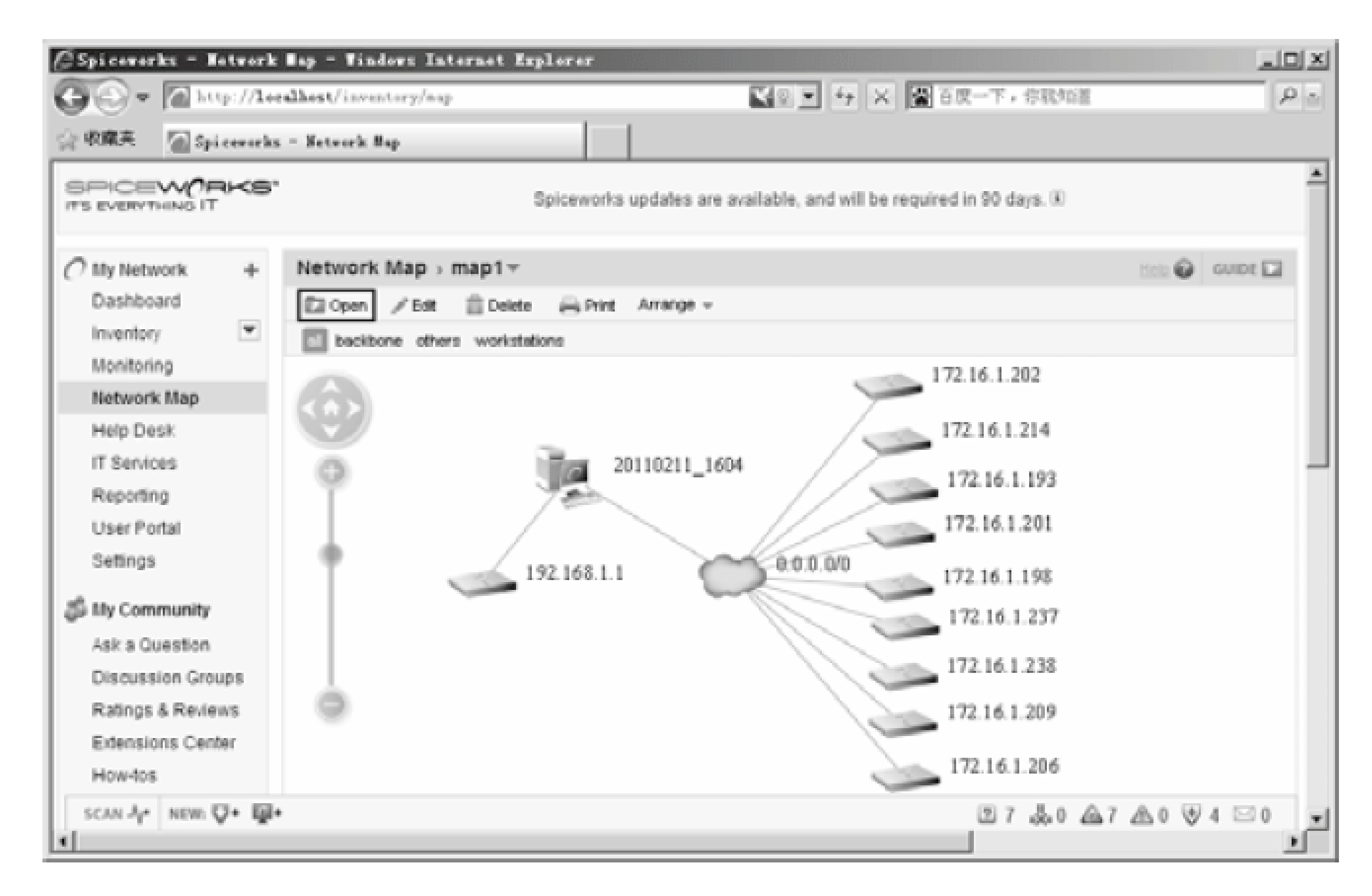


图 5-36

10 弹出【Open a map】（打开一个地图）页面，选中网络拓扑图名，单击【Open】（打开）按钮即可打开选中的网络模块，如图 5-37 所示。

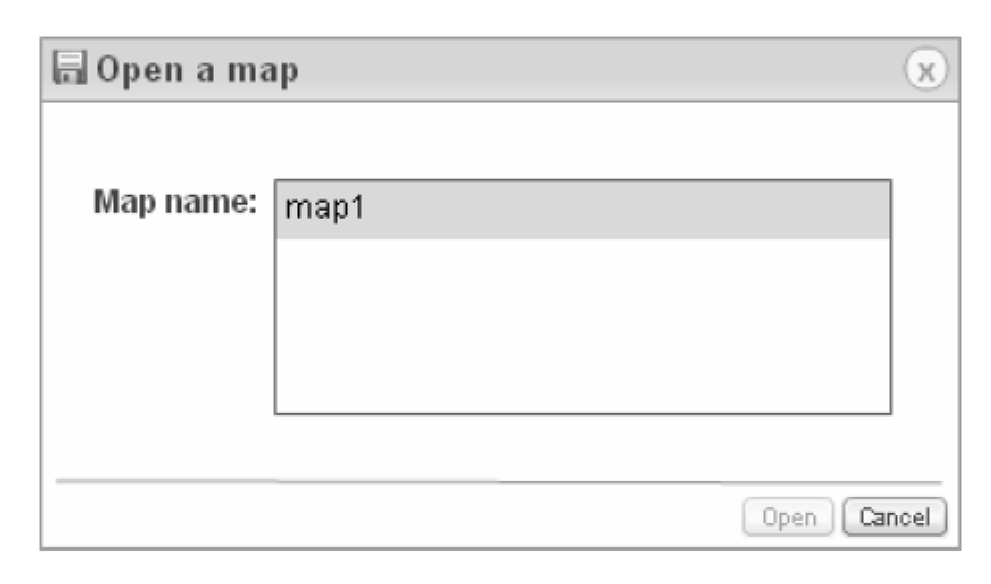


图 5-37

5.2.3　应用网管平台

Spiceworks 软件的管理功能比较多，如设备信息查看、管理日志、仪表盘快速浏览管理信息等，下面介绍几种常用的功能。

1. 设置 Spiceworks 仪表盘，直观高效地查看网络管理信息

为了方便多种管理信息的查看，Spiceworks 设定了仪表盘模块，具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择【Dashboard】（仪表板）选项，如图 5-38 所示。



图 5-38

02 在弹出的页面中单击【Add Content】（添加模块）超级链接，弹出【Add Content】模块选项列表，单击需要显示的模块的超级链接，即可添加模块到仪表盘页面，如图 5-39 所示。

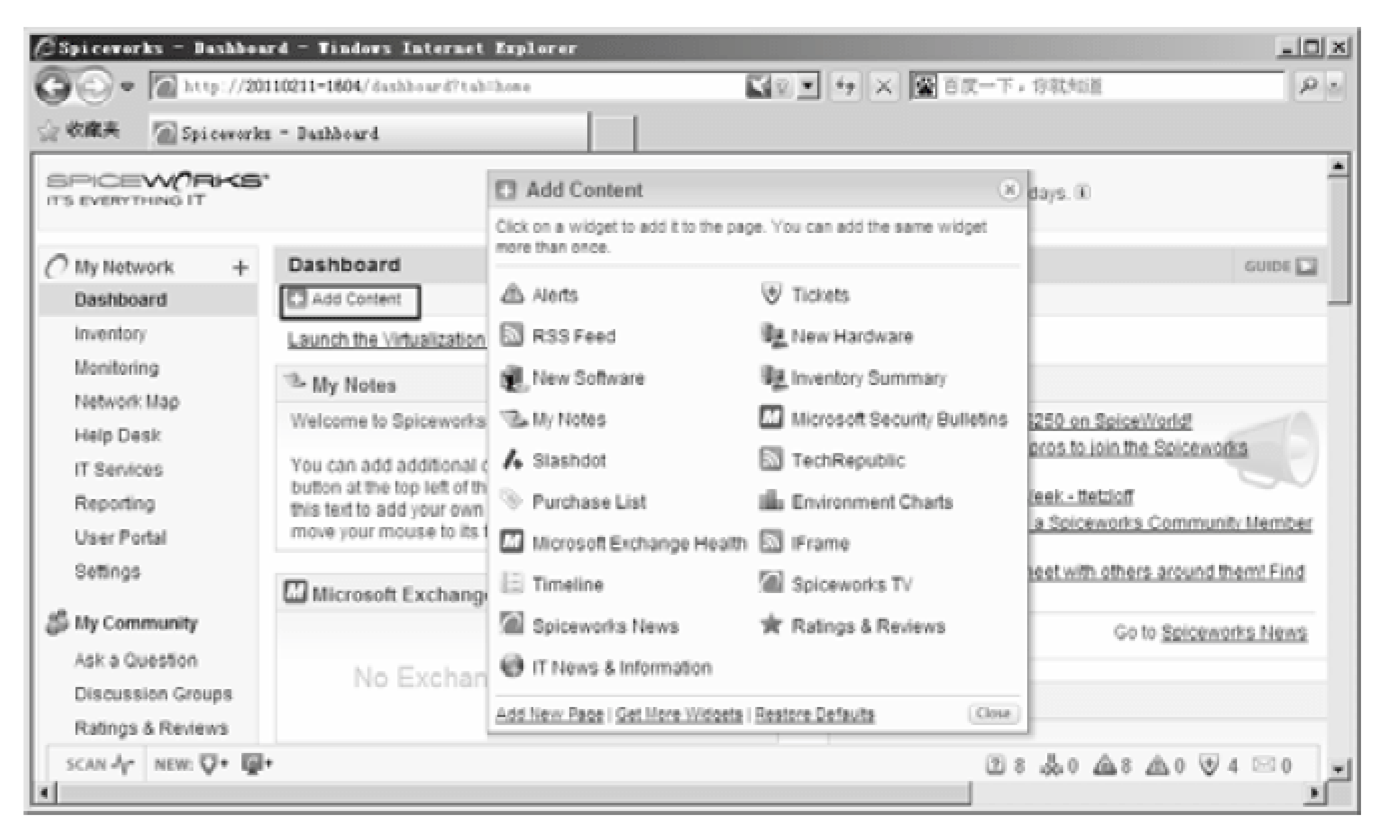


图 5-39

仪表盘中的显示模块比较多，常用模块的功能介绍如下。

（1）【Alerts】（告警）：告警模块，显示最近发生的告警信息。

（2）【New Hardware】（新硬件）：新硬件模块，显示新加网络设备。

（3）【New Software】（新软件）：新软件模块，显示新安装的软件信息。

（4）【Inventory Summary】（存货清单摘要）：设备信息摘要模块，显示现有设备。

（5）【My Notes】（我的日志）：日志模块，查看、编辑日志。

（6）【Microsoft Security Bulletins】（微软安全公告）：微软安全公告模块，显示微软发布的安全公告信息。

（7）【Timeline】（大事年表）：事件记录模块，显示 Spiceworks 网络管理平台最近发生的事件。

（8）【IT News & Information】（IT 新闻和消息）：业界新闻消息模块。

03 单击【Remove】（移除）选项，可以移除指定模块，如图 5-40 所示。

图 5-40

2. 使用 Inventory 设备清单模块，查看设备详细信息

通过 Inventory 模块，可以查看设备的详细信息，具体操作步骤如下。

01 在 Spiceworks 主界面的左侧选项列表中选择【Inventory】（库存清单）选项，右侧窗格中显示出已有设备清单，如图 5-41 所示。



图 5-41

02 如果要查看某一设备的详细信息，可以进入该设备的类别中进行查看，本实例通过查看某主机设备的信息为例进行讲解，单击【Workstations】（工作站）对象类别图标，如图 5-42 所示。



图 5-42

03 在右侧窗格中显示【Workstations】（工作站）对象类别的设备列表，单击要查看的主机设备图标，显示该设备的详细信息，如图 5-43 所示。



图 5-43

04 在页面的下方显示出对象的详细信息，默认显示【General Info】（常规信息）选项卡，如图 5-44 所示。



图 5-44

05 选择【Timeline】（大事年表）选项卡，查看该对象的操作记录，如图 5-45 所示。

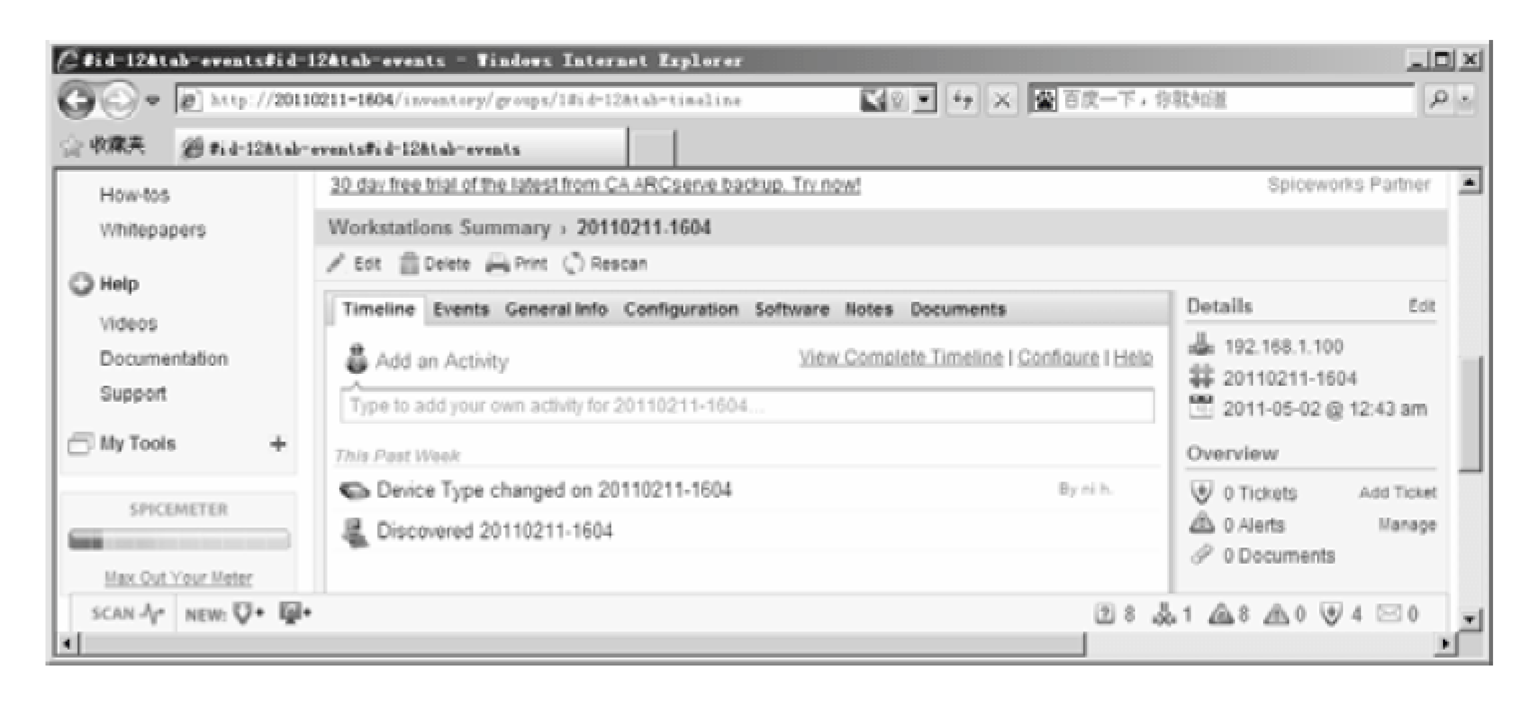


图 5-45

06 选择【Events】（事件）选项卡，查看该对象的事件记录信息，如图 5-46 所示。

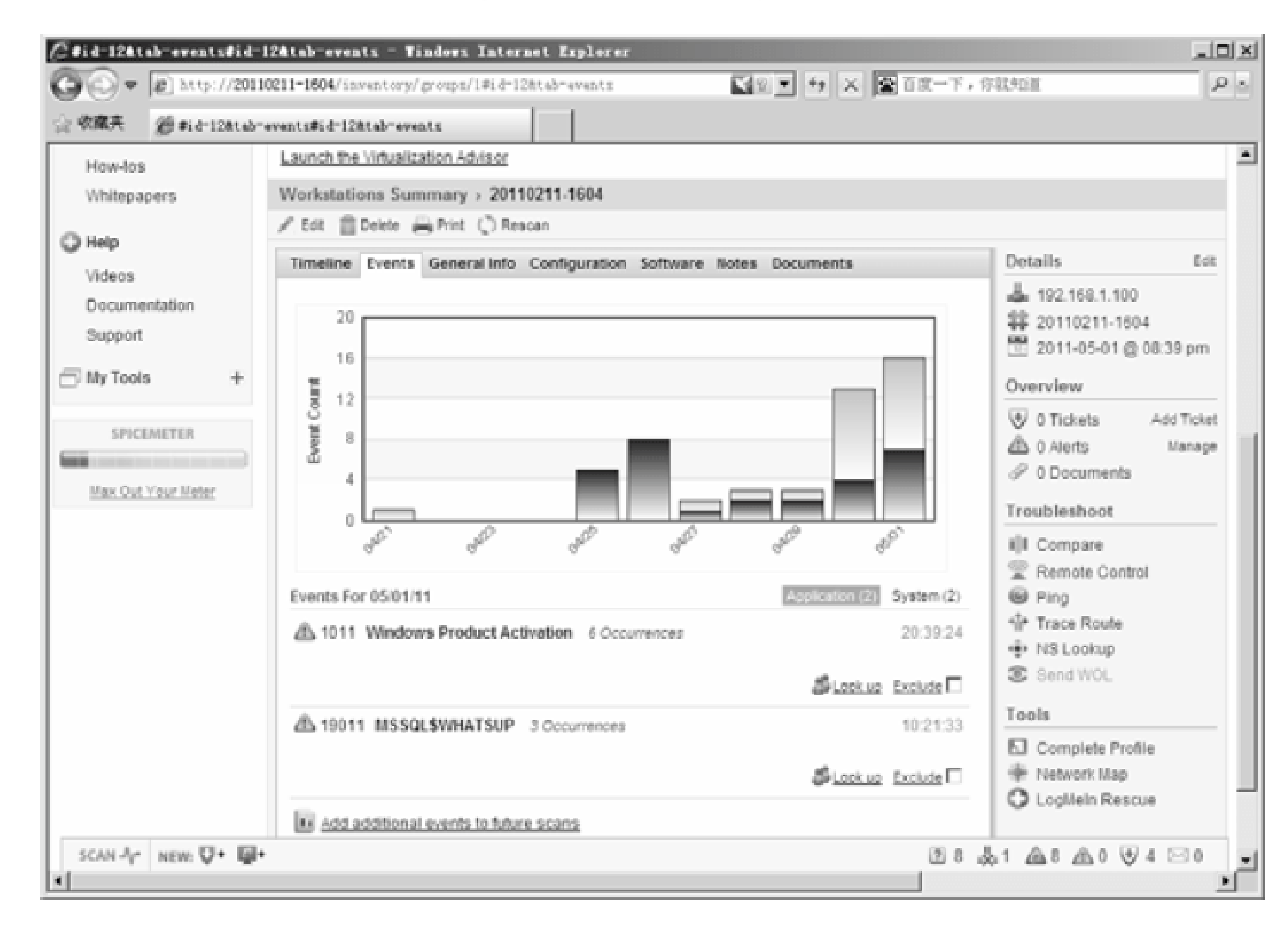


图 5-46

07 选择【Configuration】(配置)选项卡，查看该对象的配置信息，如图 5-47 所示。

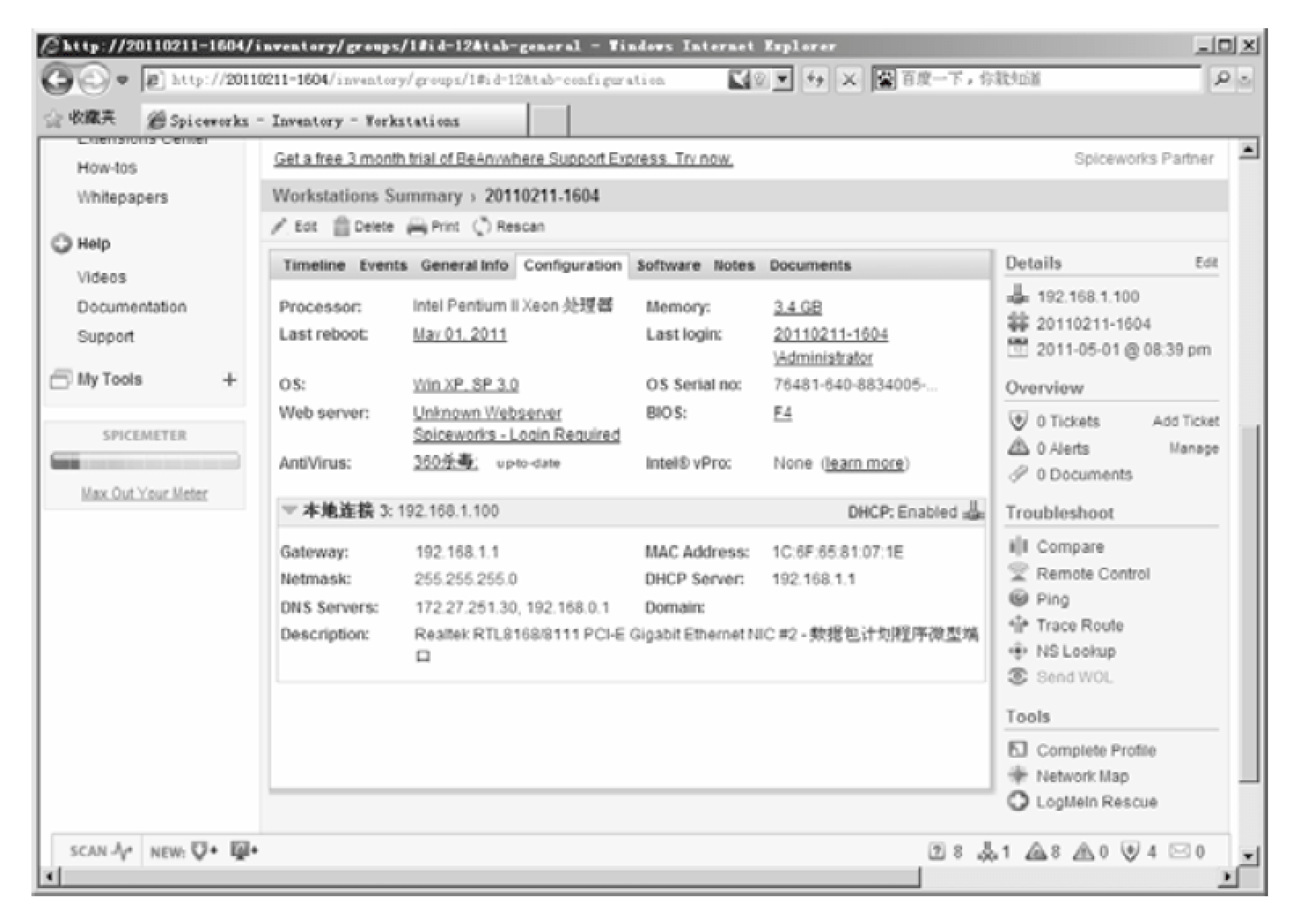


图 5-47

08 选择【Software】选项卡，查看该主机安装的软件信息，单击【Edit】（编辑）按钮，如图 5-48 所示。

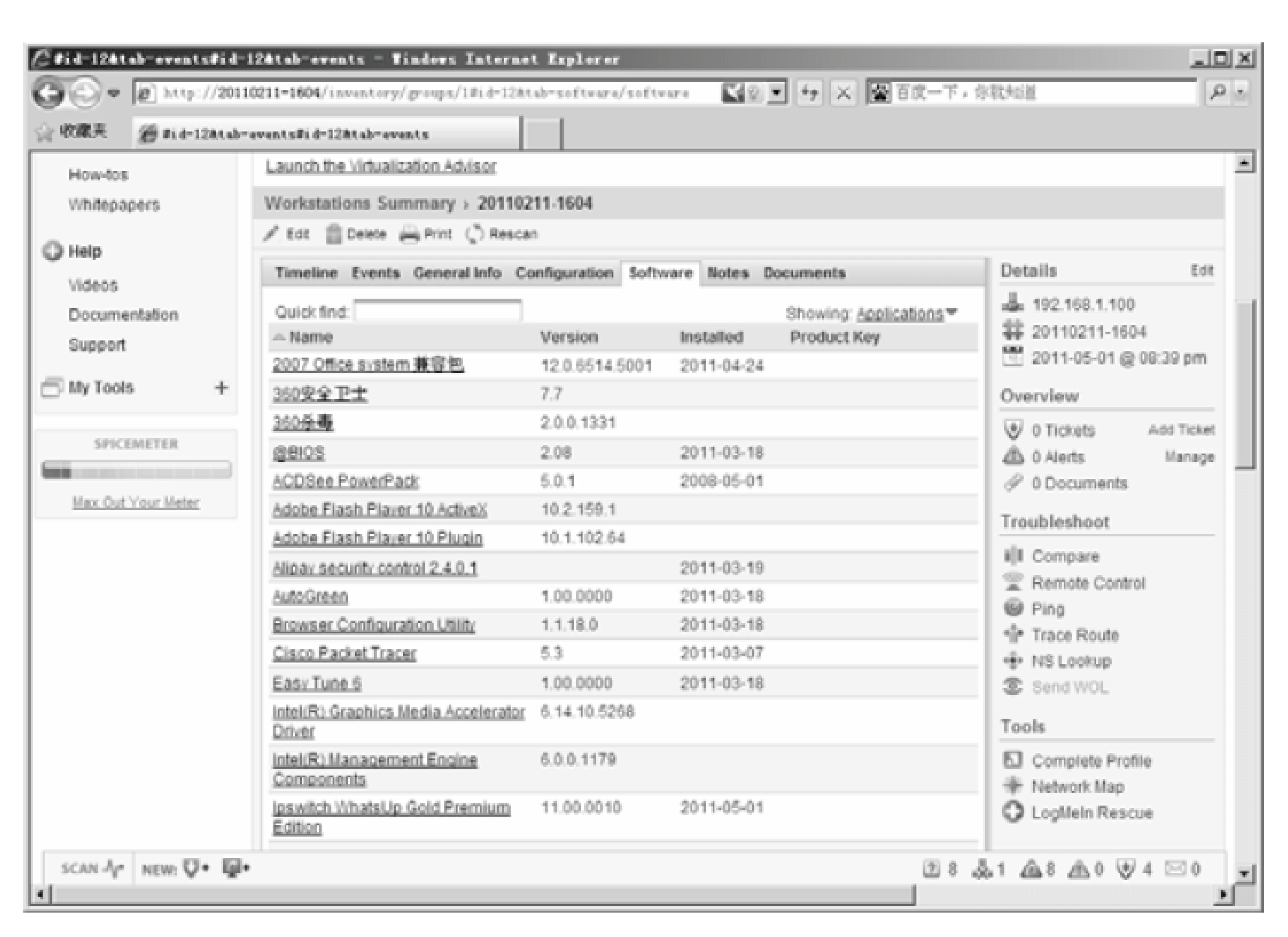


图 5-48

09 进入对象编辑界面，可以编辑该对象的部分信息，如图 5-49 所示。

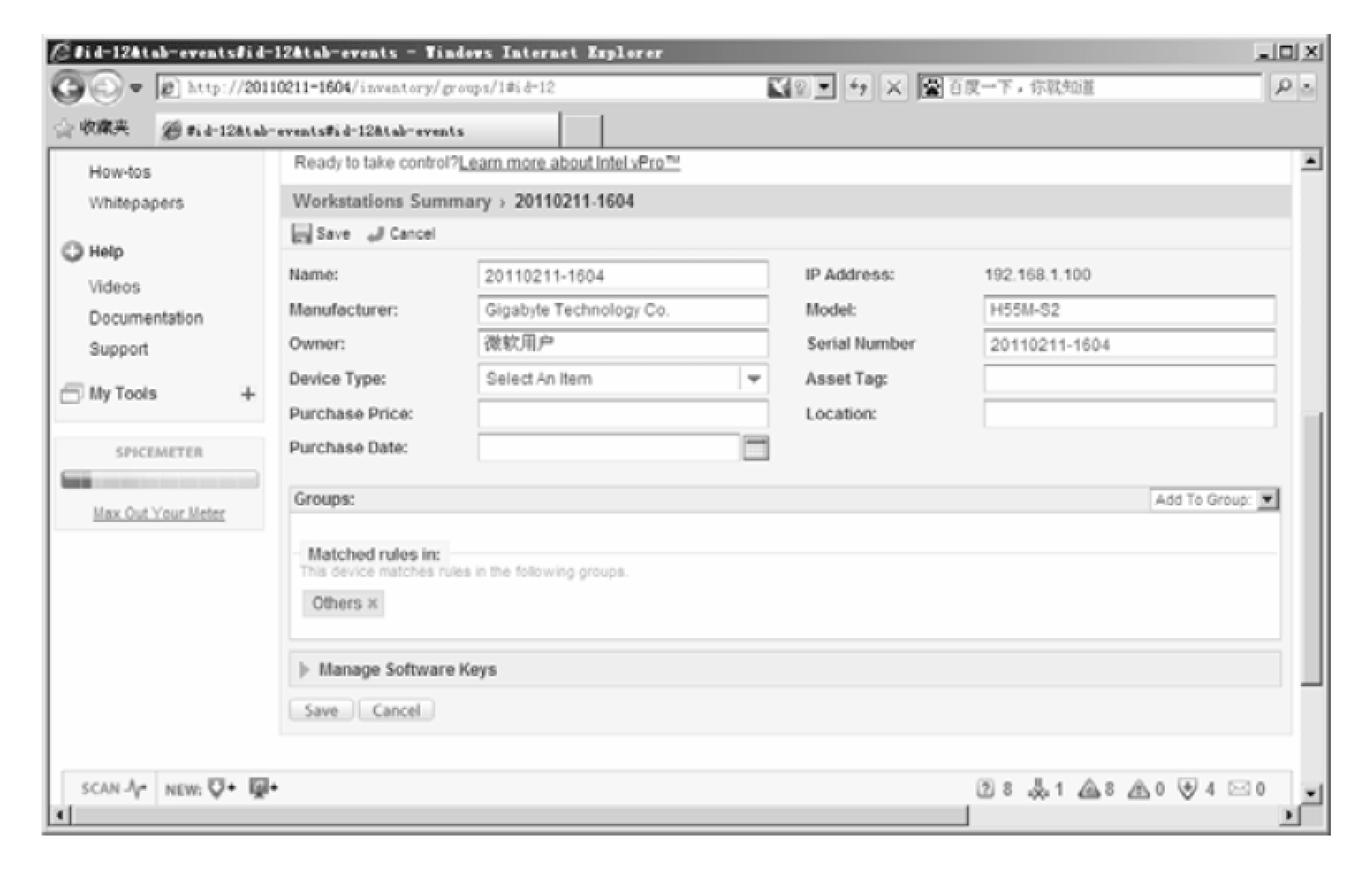


图 5-49

信息查看还有另一种界面可选，具体操作步骤介绍如下。

01 选择【Icon View】（图示视图）➢【Browse View】（浏览视图）菜单命令，如图 5-50 所示。



图 5-50

02 进入对象信息显示界面，可以查看对象的详细参数信息，如图 5-51 所示。

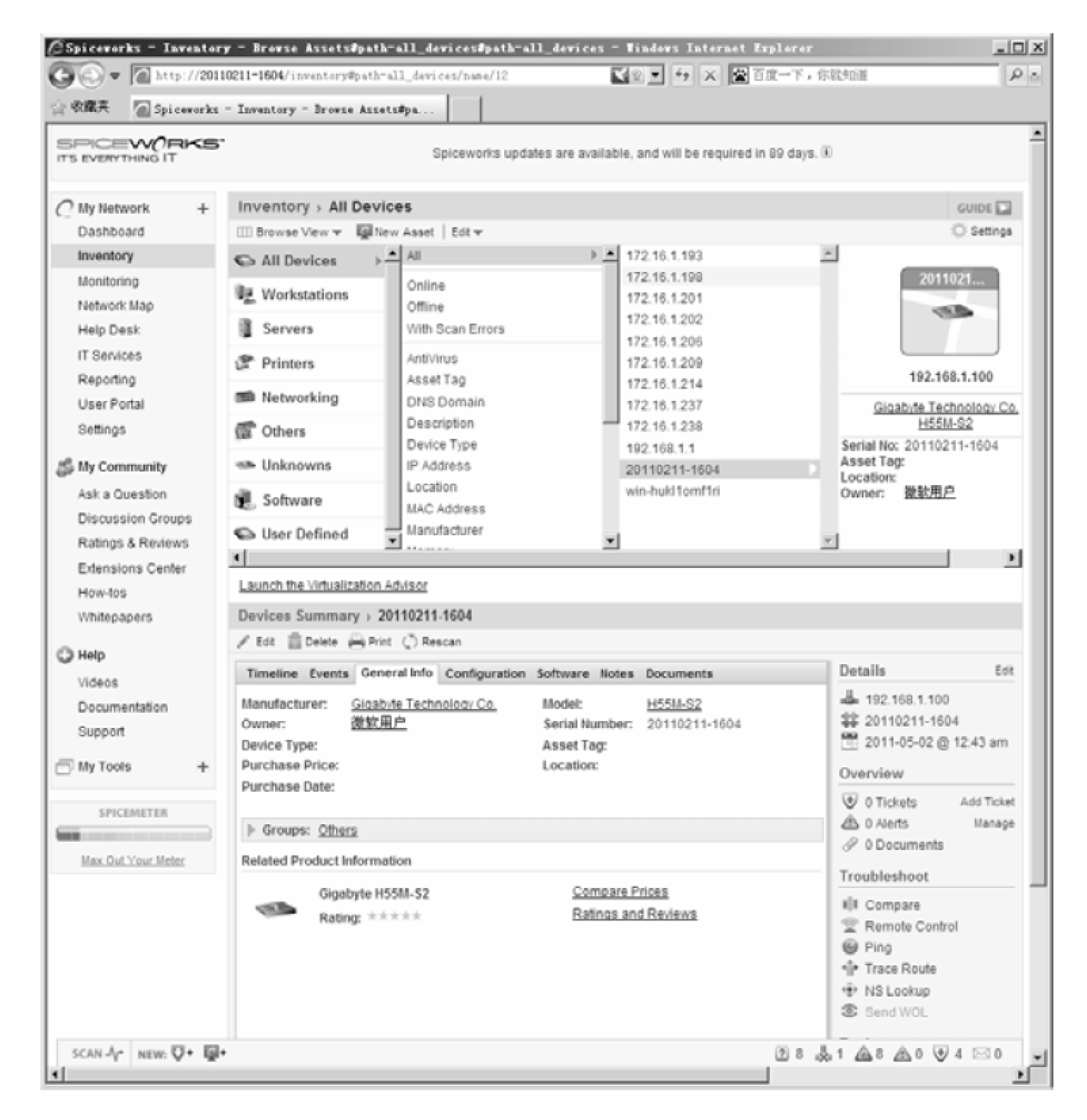


图 5-51

3. 扫描新添加的网络

在网络中有新用户或新网络添加时，需及时对新添加的设备或网段进行扫描，具体操作步骤如下。

01 选择 Spiceworks 界面左侧选项列表中的【Settings】（设置选项）选项，并单击右侧窗口中的【Network Scan】（网络扫描）按钮，如图 5-52 所示。

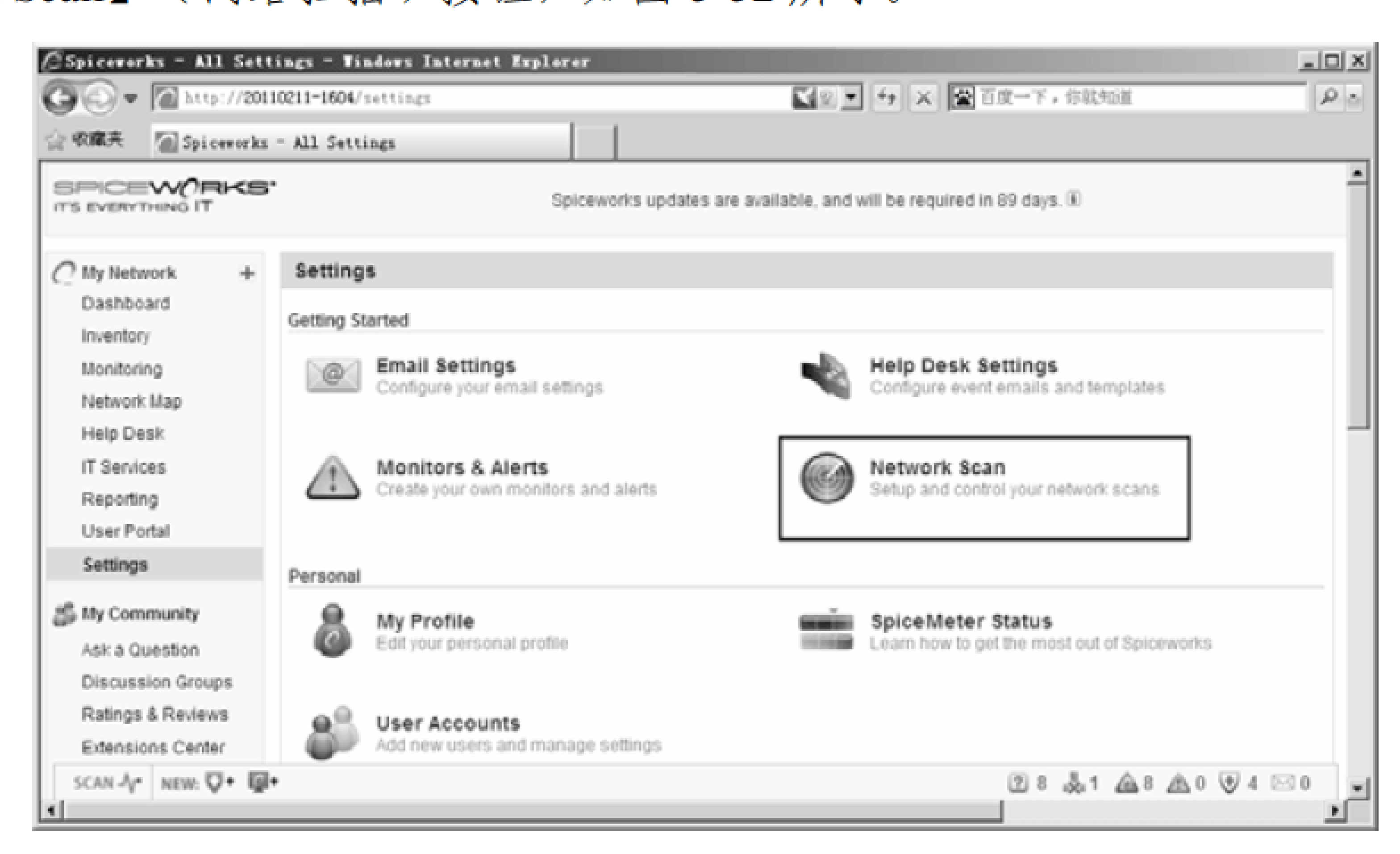


图 5-52

02 进入【Network Scan】（网络扫描）界面，单击【Click here to add a new scan entry】（单击这里添加新扫描网络）选项，添加新网络并进行扫描，如图 5-53 所示。

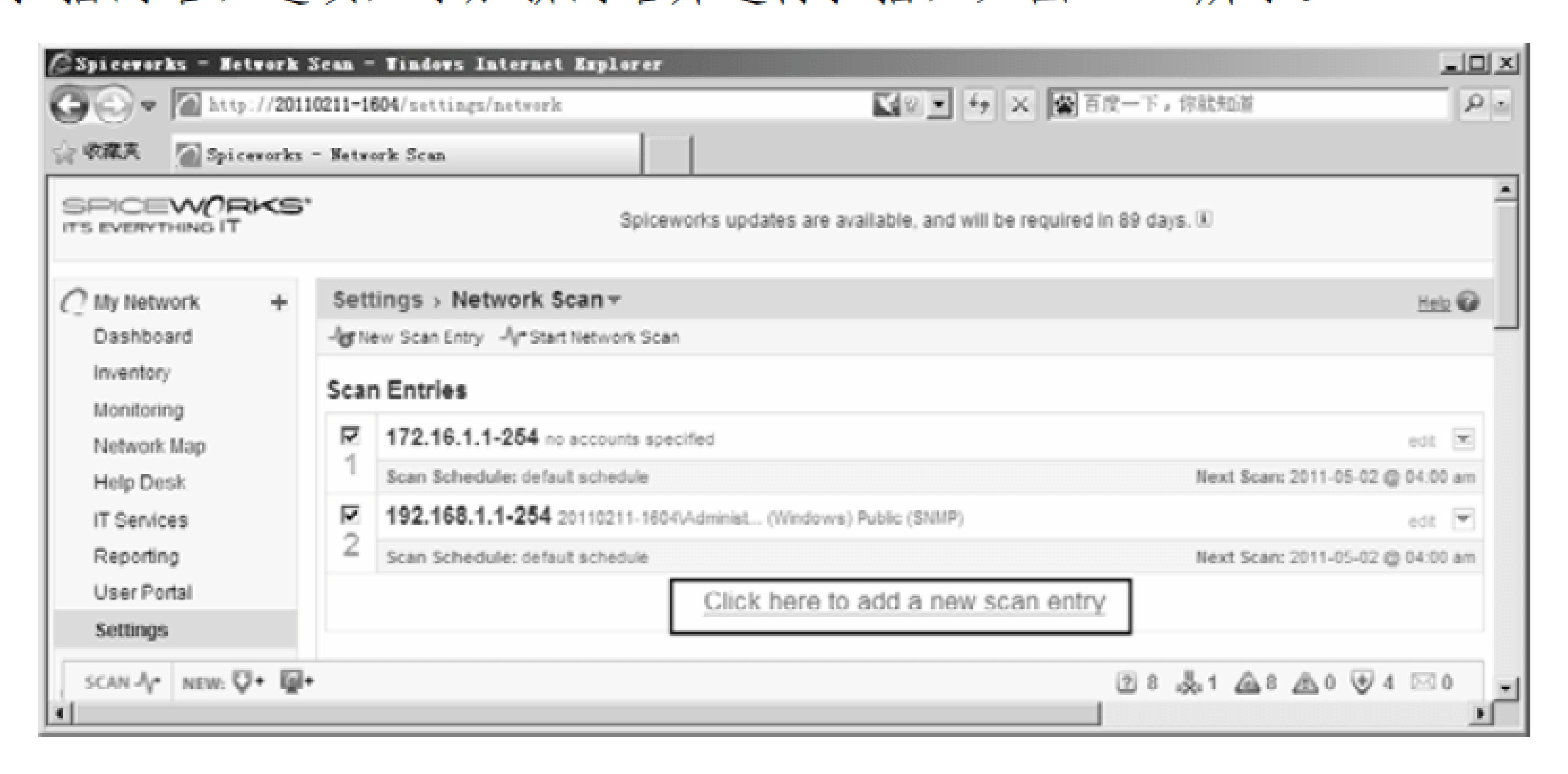


图 5-53

5.3　项目实施 2：搭建 WhatsUp Gold 网络管理平台

WhatsUp Gold 软件也是一款功能完善的网络管理软件，它与 Spiceworks 软件的功能及实现流程相似。下面主要介绍 WhatsUp Gold 网络管理平台的搭建及应用方法。

5.3.1　架设网络管理平台

WhatsUp Gold 与 Spiceworks 的环境要求相似，但是具体的操作方法不同。安装 WhatsUp Gold 的具体操作步骤如下。

01 运行安装程序，弹出【Welcome】（欢迎）对话框，单击【Next】（下一步）按钮，如图 5-54 所示。

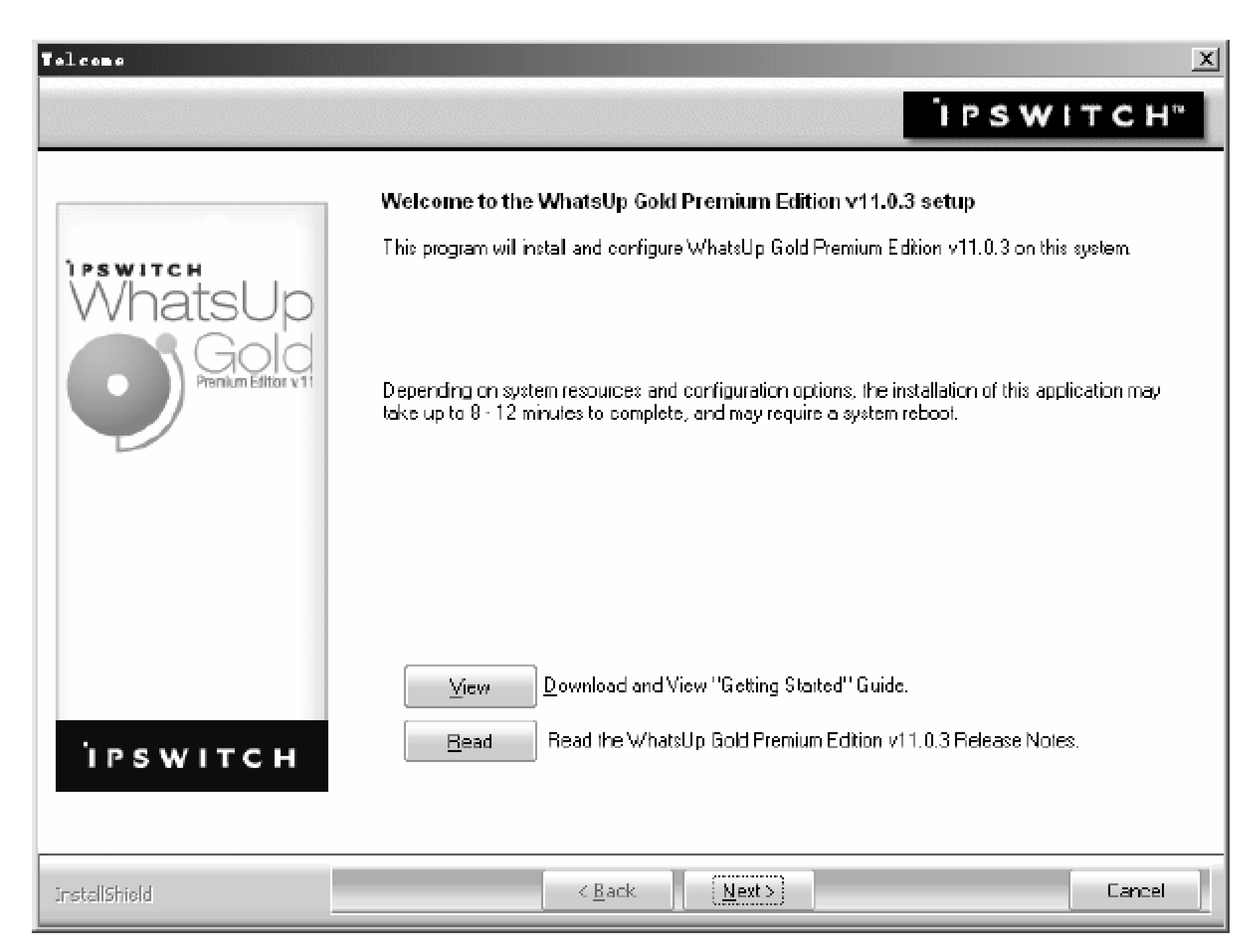


图 5-54

02 弹出【License Agreement】（许可协议）对话框，选择【I accept the terms of the license agreement】（接受许可协议）复选框，单击【Next】（下一步）按钮，如图 5-55 所示。

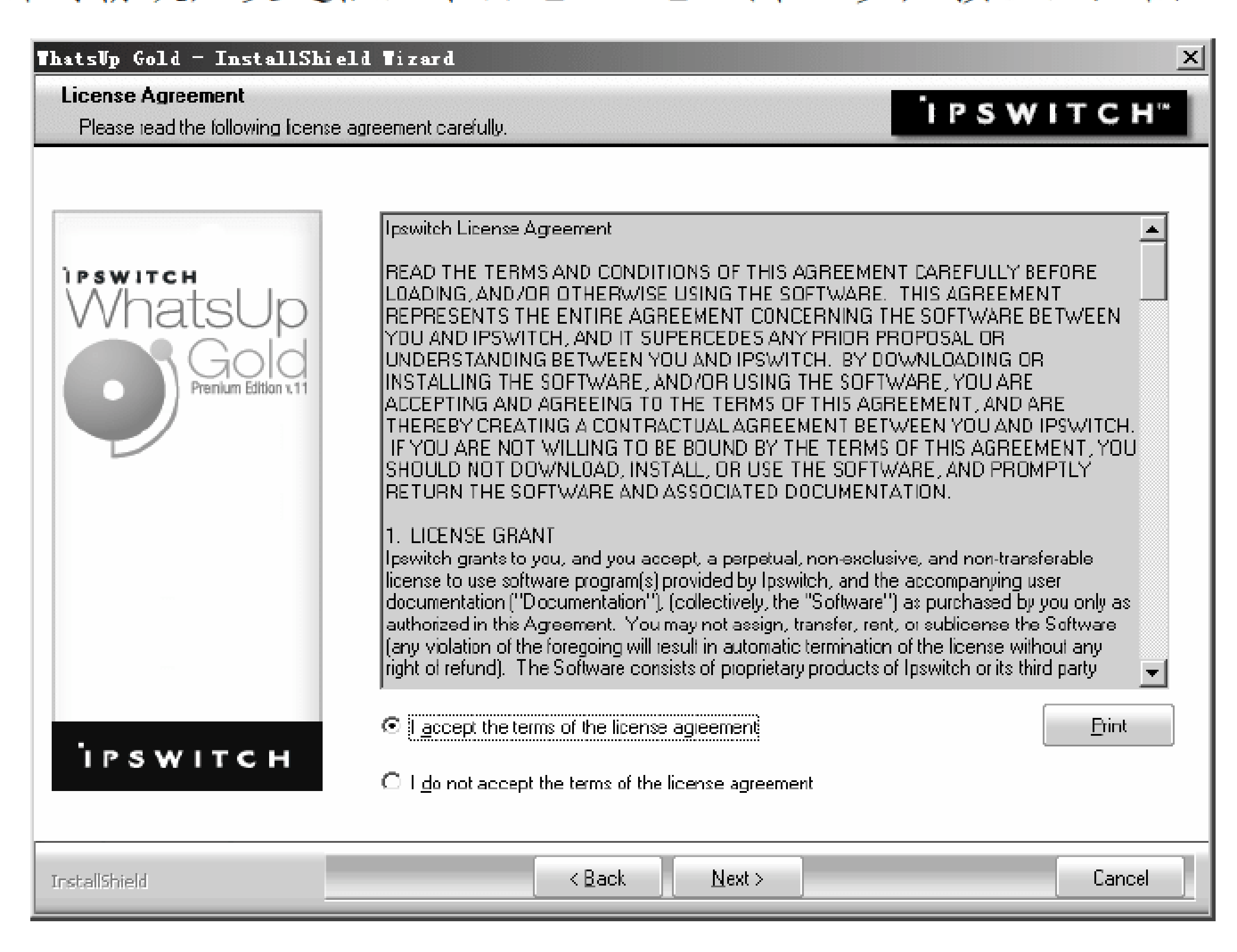


图 5-55

03 弹出【Enter MSDE-2000 Server Paths】（Mictosoft 数据库服务器路径）对话框，单击【Browse】（浏览）按钮，可以设置数据库文件存放的位置，本实例采用默认配置，单击【Next】（下一步）按钮，如图 5-56 所示。

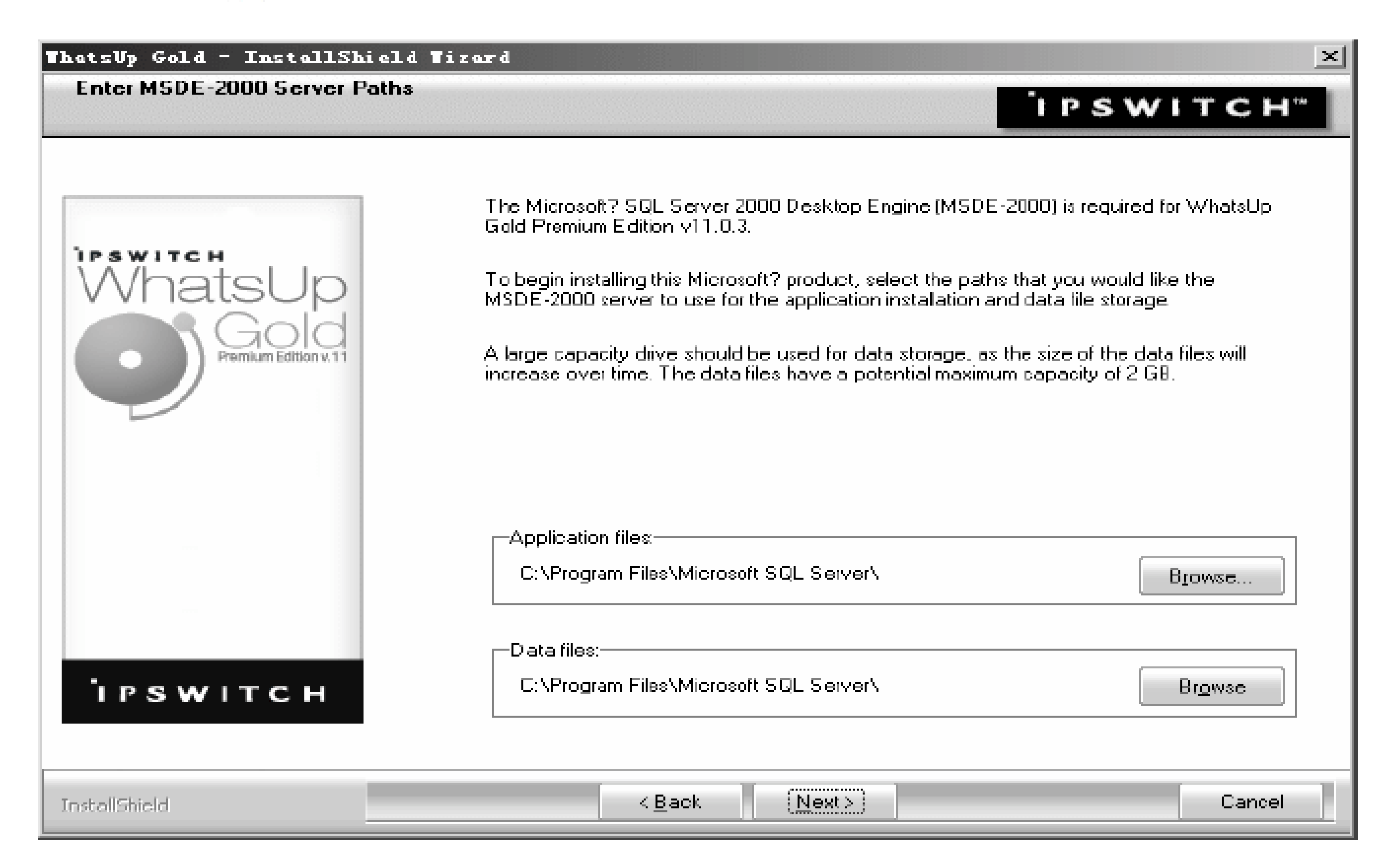


图 5-56

04 弹出【Choose Destination Location】（更改目录位置）对话框，单击【Browse】（浏览）按钮，可以设置 WhatsUp Gold 软件的安装目录位置，本实例采用默认配置，单击【Next】（下一步）按钮，如图 5-57 所示。

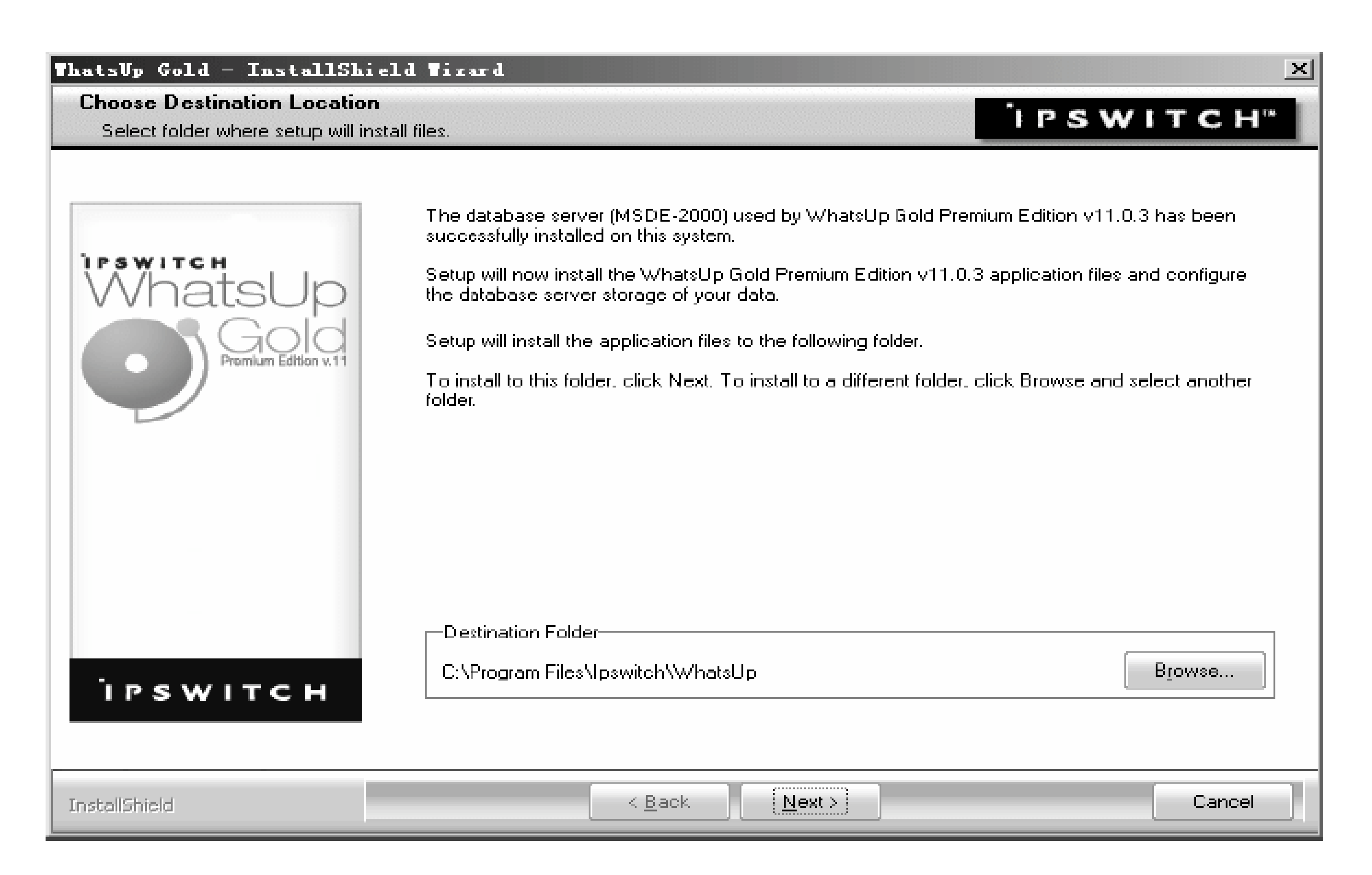


图 5-57

05 弹出【Enable Web Server】（设置 Web 服务）对话框，选择【Yes】（是）复选框，开启 WhatsUp Gold 服务器的 Web 访问功能，在【Enable Web server on port】（设置 Web 服务端口）文本框中输入 Web 连接端口，本实例采用默认配置“80”端口，单击【Next】（下一步）按钮，如图 5-58 所示。

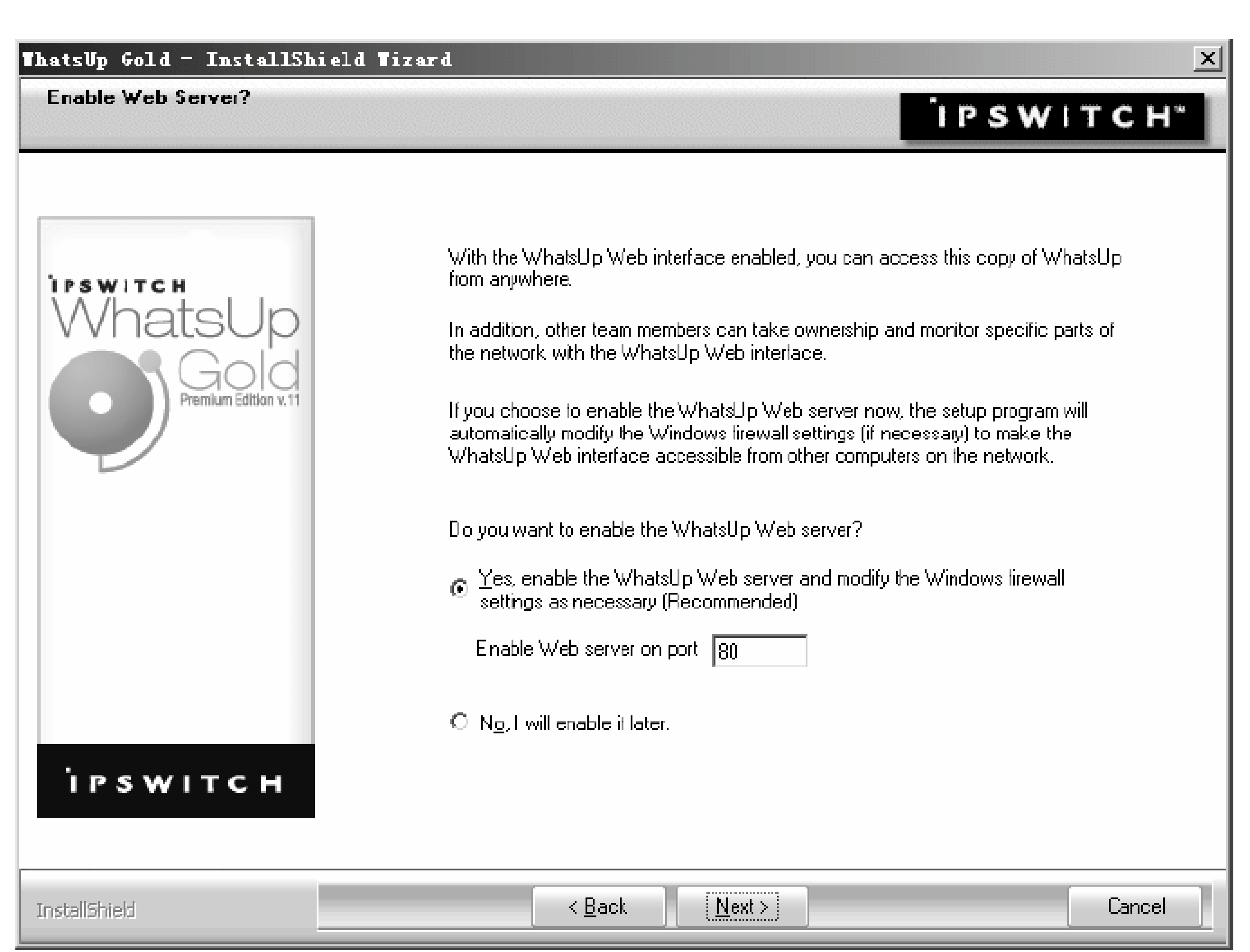


图 5-58

06 弹出【Ready to Install the Program】（准备安装程序）对话框，单击【Install】（安装）按钮，如图 5-59 所示。

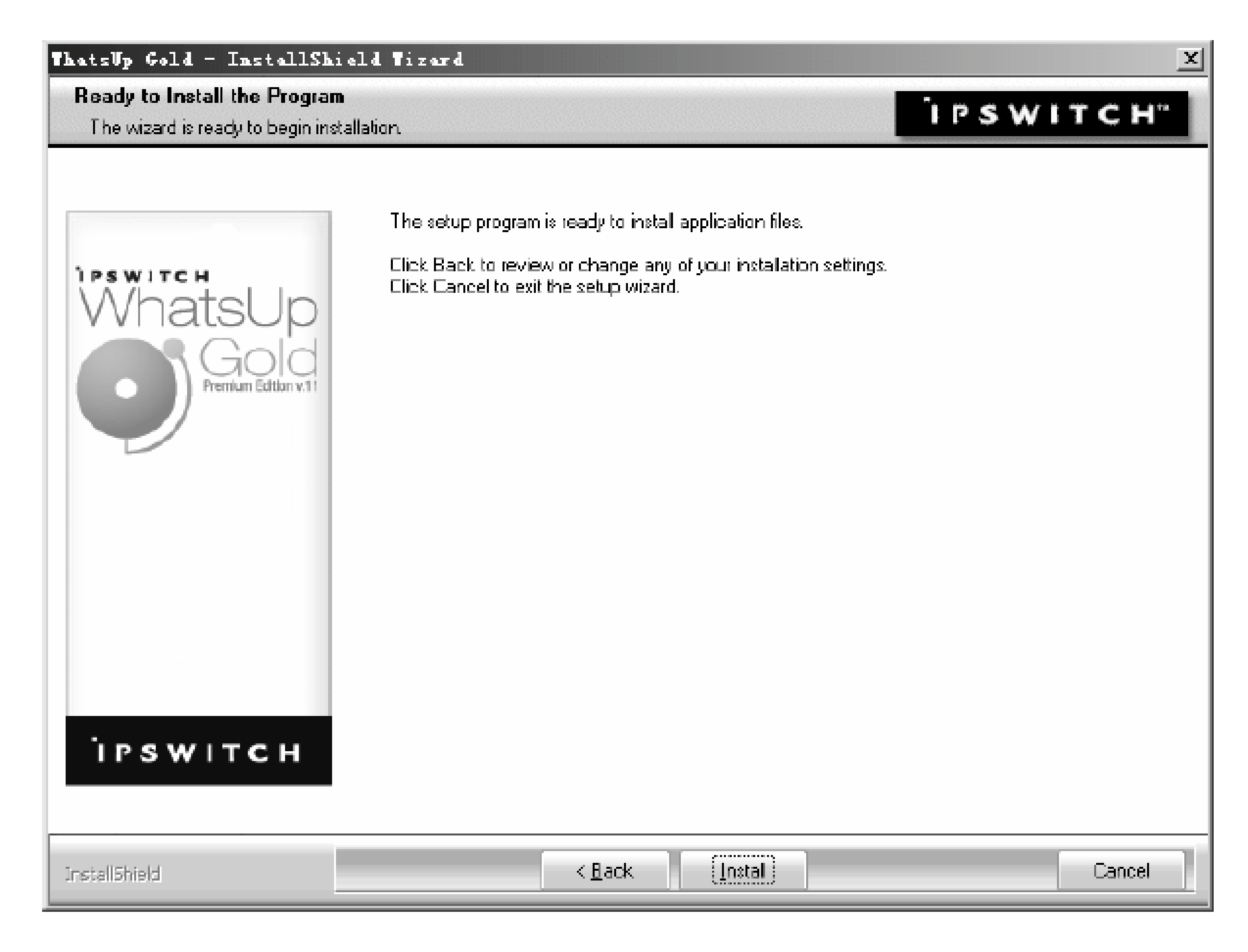


图 5-59

07 系统开始自动安装 WhatsUp Gold，并显示安装的进度，如图 5-60 所示。

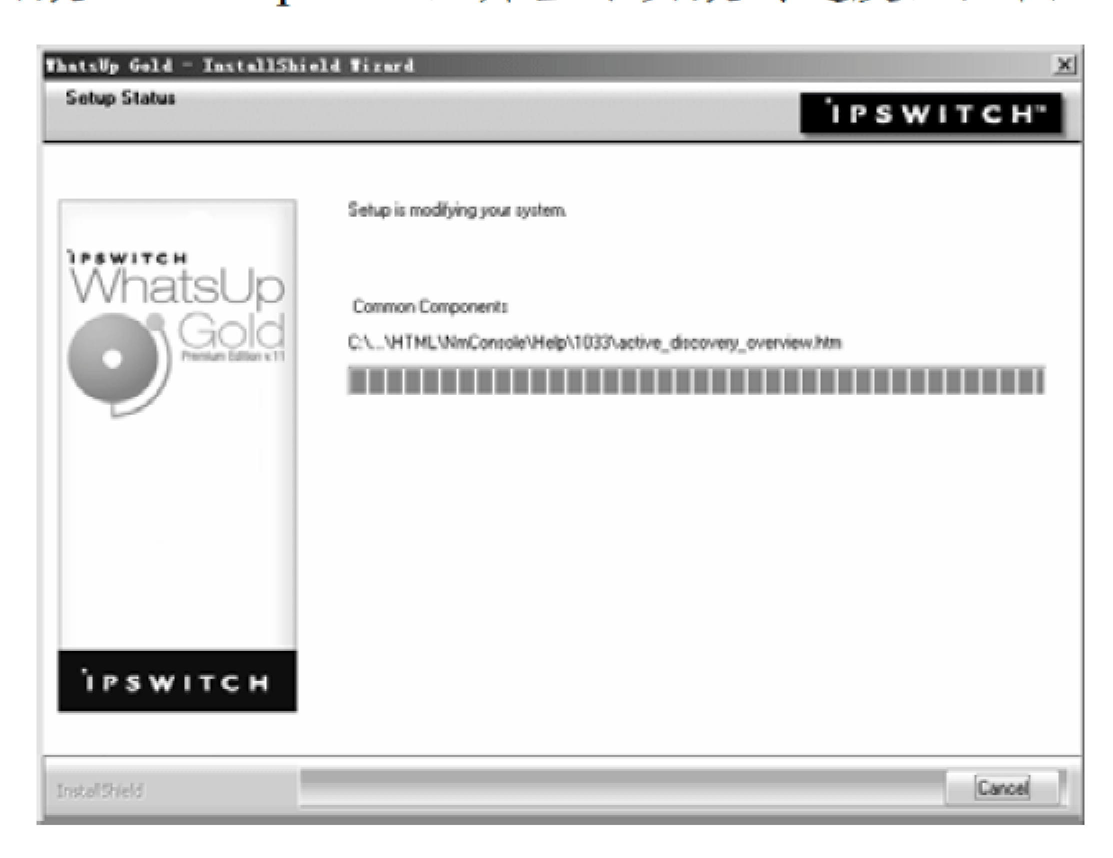


图 5-60

08 WhatsUp Gold 安装完成后，单击【Finish】（完成）按钮，如图 5-61 所示。

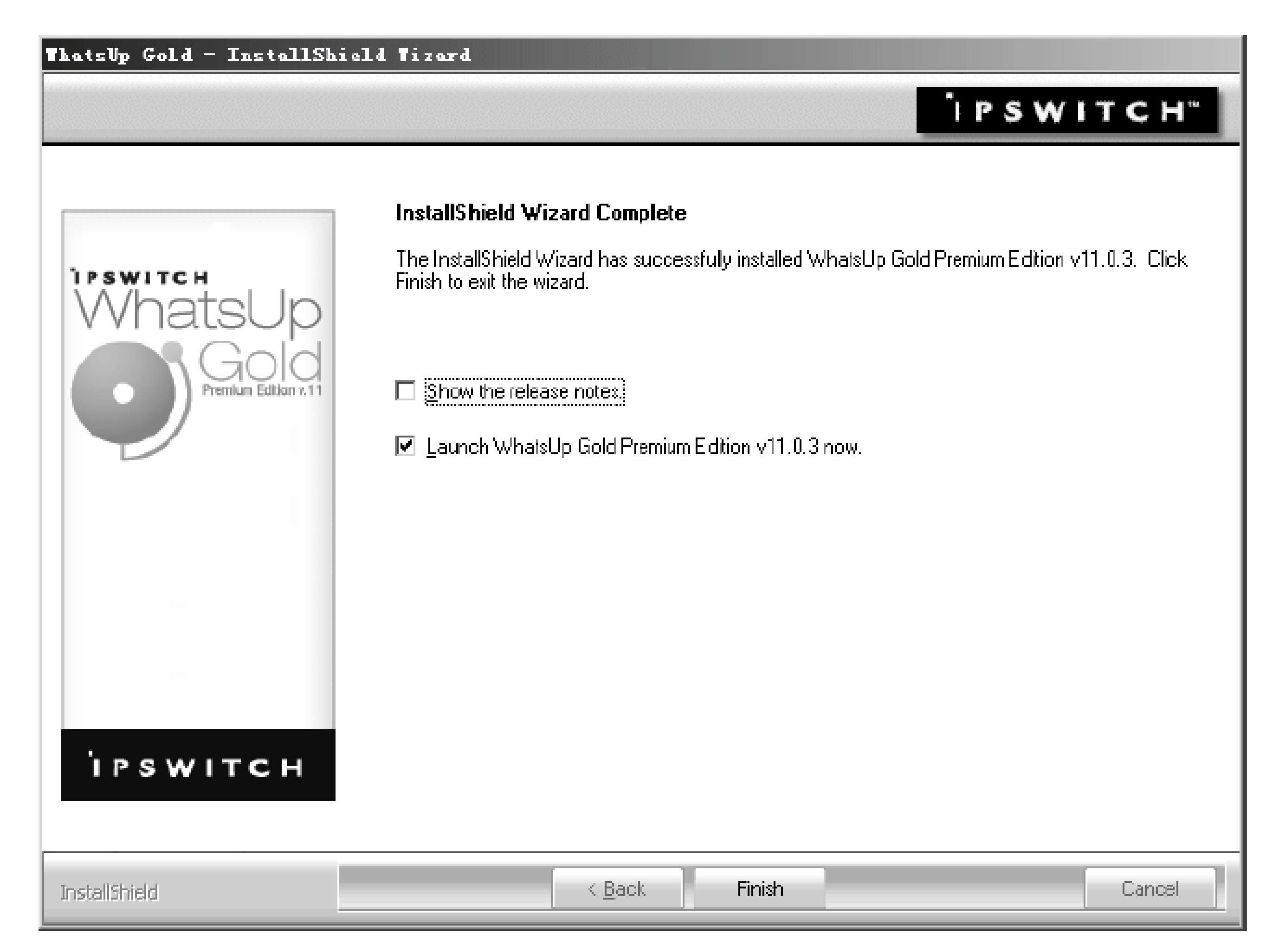


图 5-61

09 系统自动弹出软件激活对话框，选择【Activate Later】（稍后激活）复选框，单击【下一步】按钮，如图 5-62 所示。到这一步，系统已经安装成功。

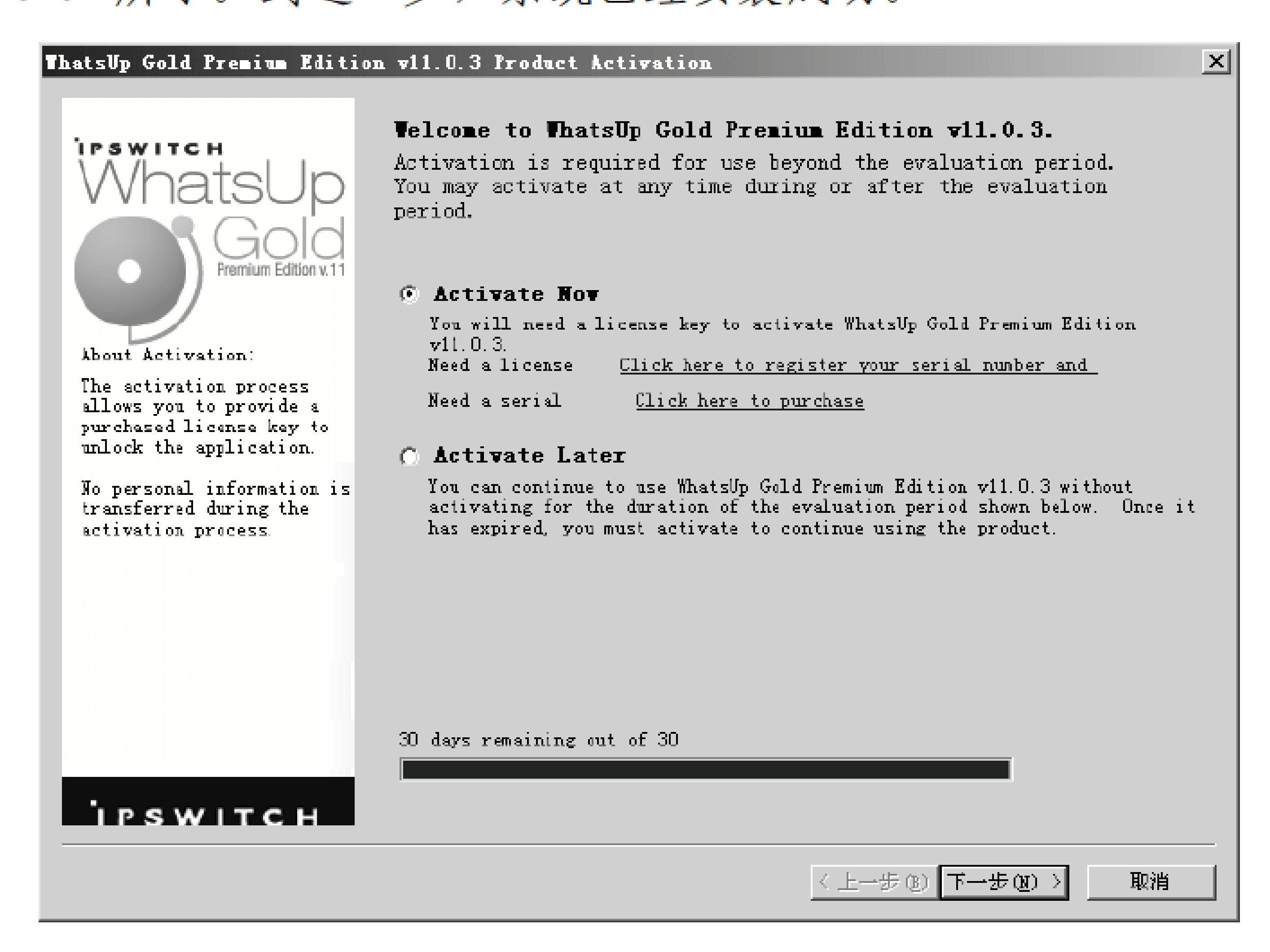


图 5-62

5.3.2 实现网络环境监控

使用 WhatsUp Gold 软件监视网络环境，首先要进行网络扫描，获得网络拓扑、设备配置及性能等信息，使用 WhatsUp Gold 软件获取网络拓扑的操作方法如下。

1. 第一次网络扫描

首次运行 WhatsUp Gold 软件，会弹出初次网络扫描的配置向导，使用向导可以轻松地获得第一手网络资料，具体操作步骤如下。

01 启动 WhatsUp Gold 软件，弹出【Setting up the application for the first time】对话框，单击【Next】（下一步）按钮，如图 5-63 所示。

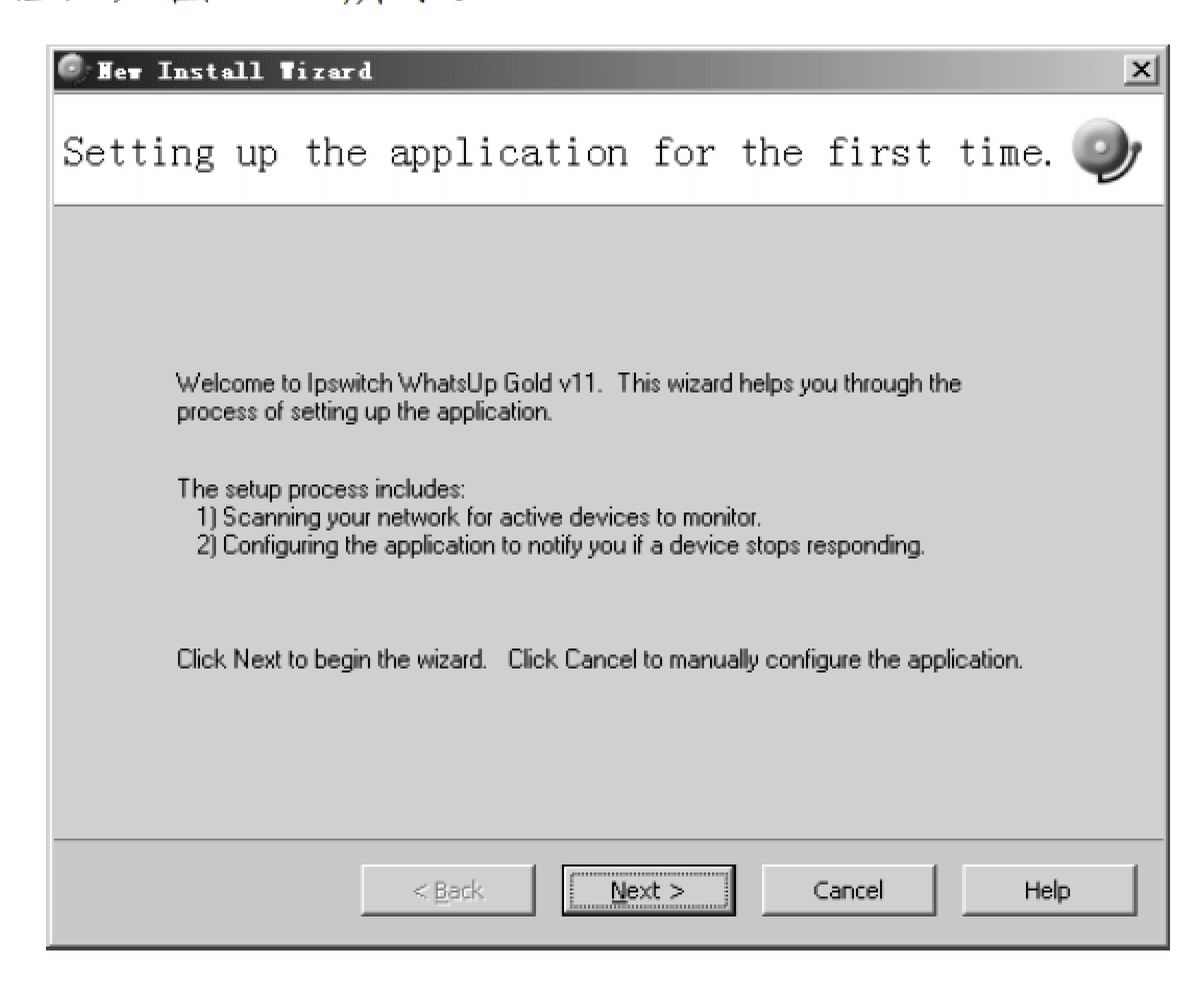


图 5-63

02 弹出【Device Discovery Methods】（设备发现方法）对话框，选择【IP range scan】（扫描 IP 组）单选按钮，单击【Next】（下一步）按钮，如图 5-64 所示。

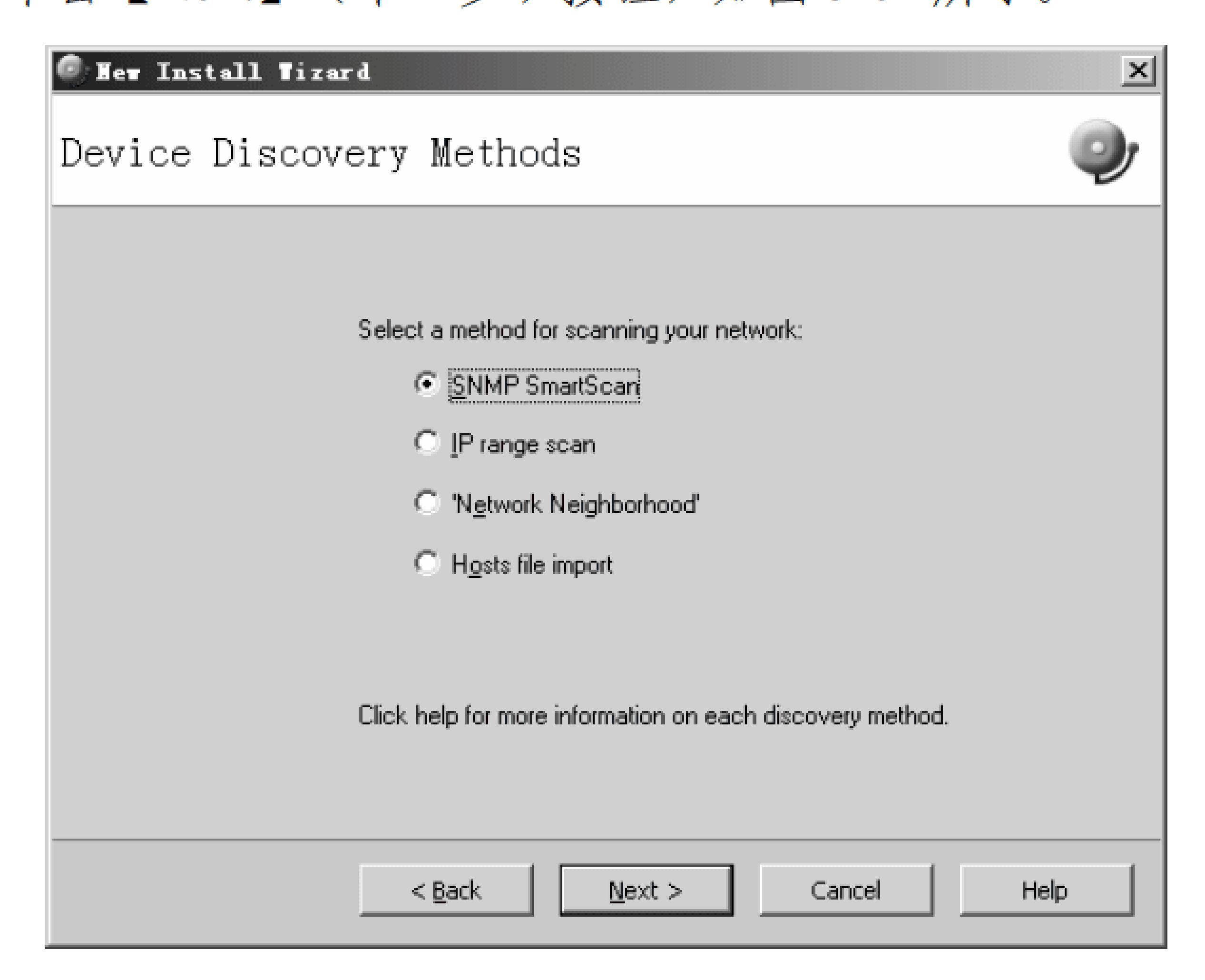


图 5-64

该对话框各个参数的含义如下。

（1）【SNMP SmartScan】（SNMP 精确扫描）：使用 SNMP 网络管理协议扫描，以团体名为扫描依据。

（2）【IP range scan】（IP 组扫描）：针对指定 IP 地址范围进行扫描。

（3）【'Network Neighborhood'】（网络邻居）：扫描网络邻居。

（4）【Hosts file import】（主机文件导入）：依照 Hosts 文件列表进行扫描。

03 弹出【IP Range to Scan】（使用 IP 组扫描）对话框，在【Start address】（起始地址）文本框中输入起始扫描地址，在【End address】（结束地址）文本框中输入终止扫描地址，单击【Next】（下一步）按钮，如图 5-65 所示。

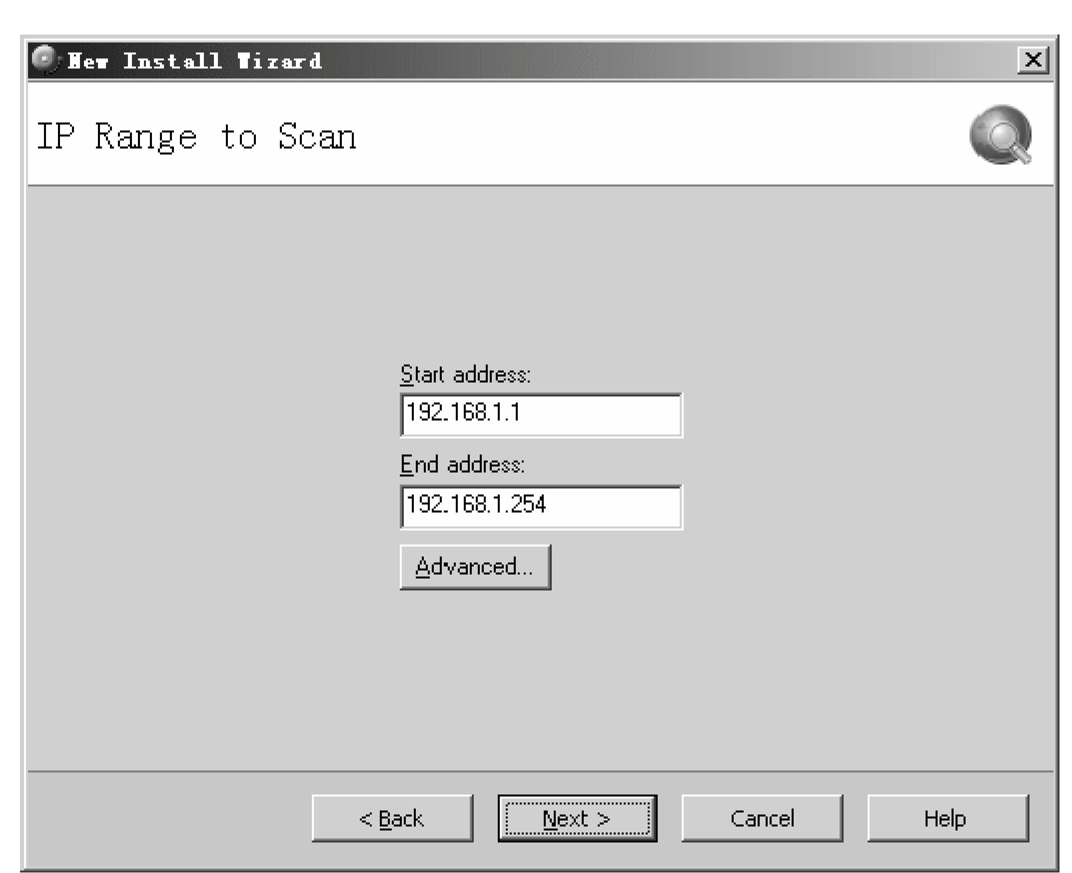


图 5-65

04 弹出【SNMP Communities】（SNMP 团体）对话框，在【SNMP read communities】（SNMP

可读团体）文本框中输入 SNMP 团体名，本实例采用默认配置“public”，单击【Next】（下一步）按钮，如图 5-66 所示。

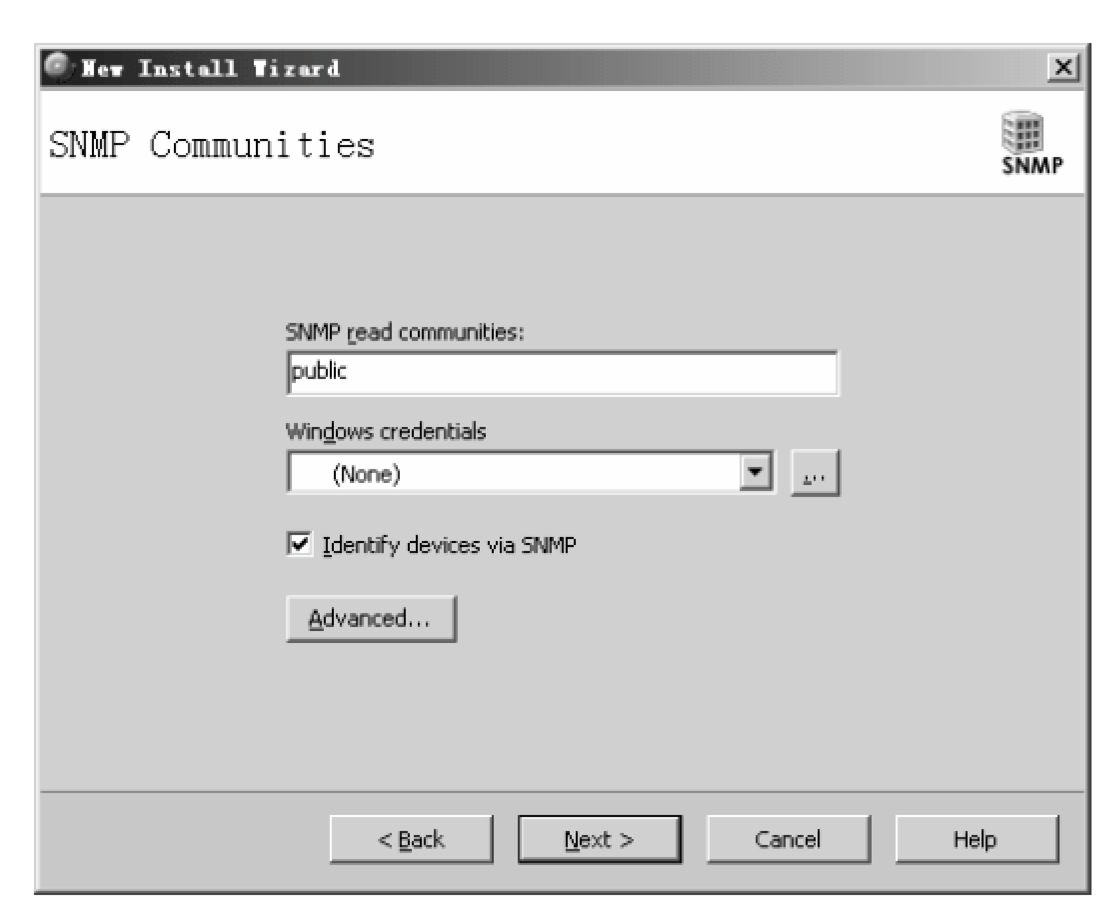


图 5-66

05 弹出【Active/Performance Monitors to Scan】（活动/性能显示扫描）对话框，设置扫描活动协议状态及设备性能信息，单击【Next】（下一步）按钮，如图 5-67 所示。

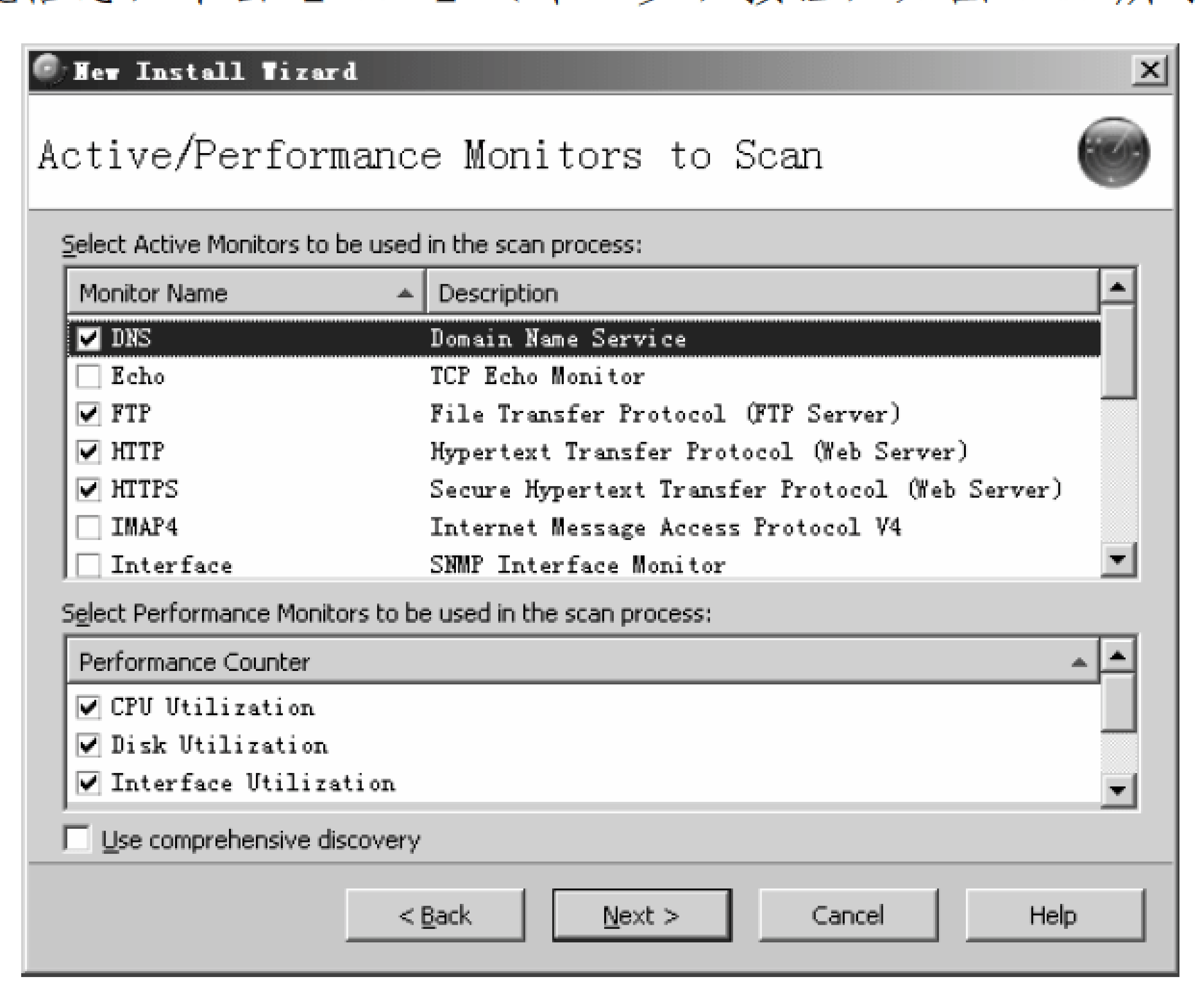


图 5-67

06 系统自动开始扫描网络，并显示扫描进度，如图 5-68 所示。

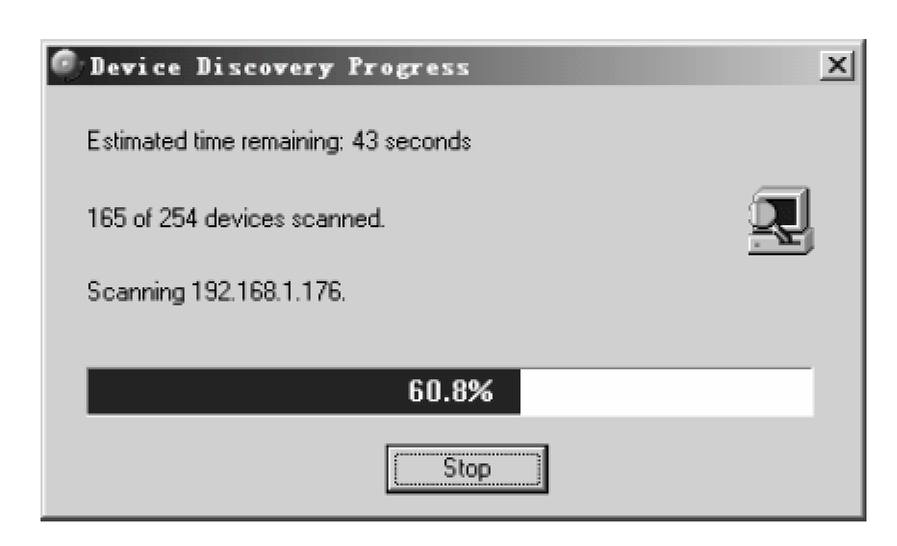


图 5-68

07 扫描结束后弹出【Devices to Monitor】（设备显示列表）对话框，显示扫描结果，选择需显示设备左侧的复选框，单击【Next】（下一步）按钮，如图 5-69 所示。

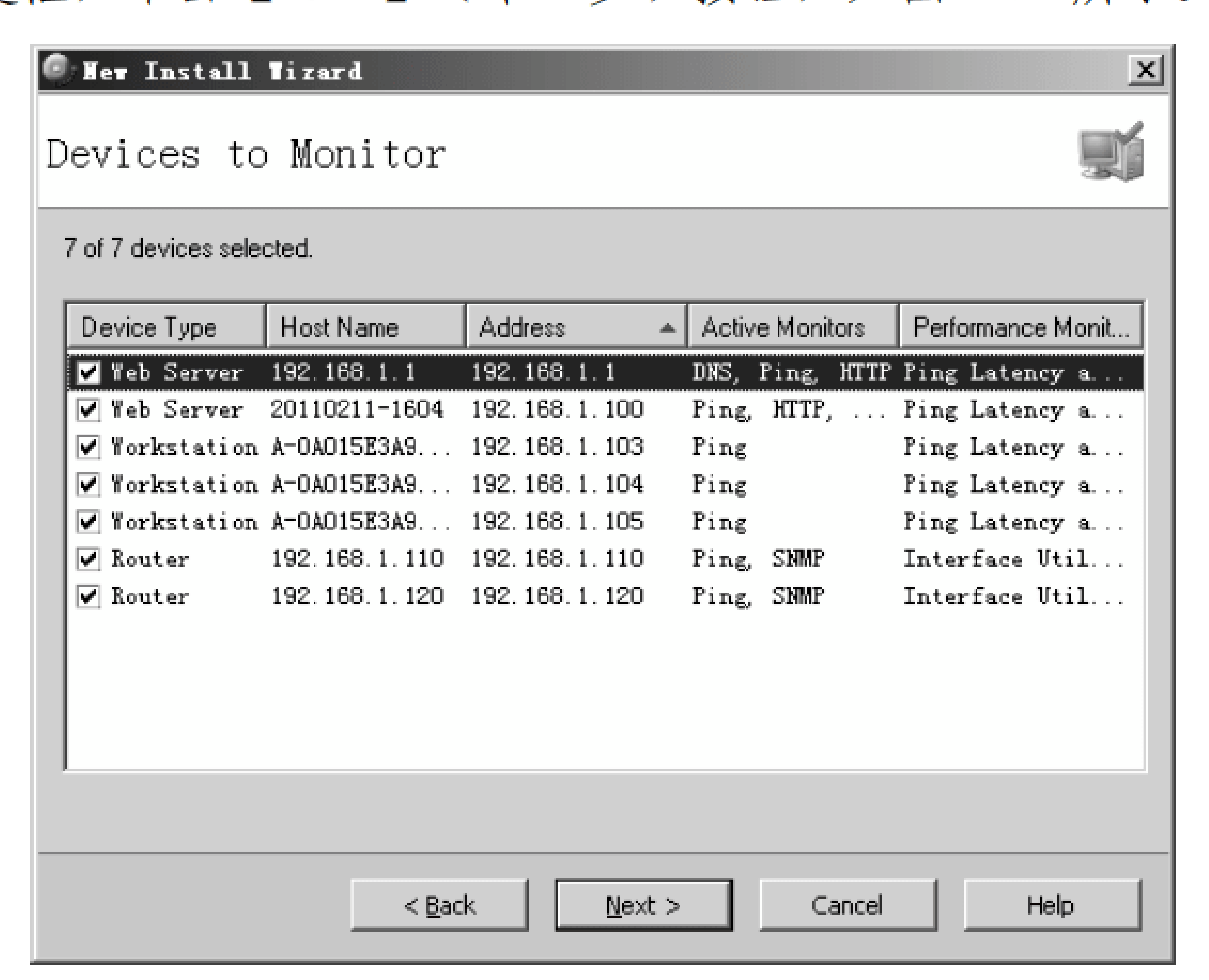


图 5-69

08 弹出【Action Policy Selection】(选择动作策略) 对话框，选择【Assist in creating a new action policy】（设置新动作策略）单选按钮，单击【Next】（下一步）按钮，如图 5-70 所示。

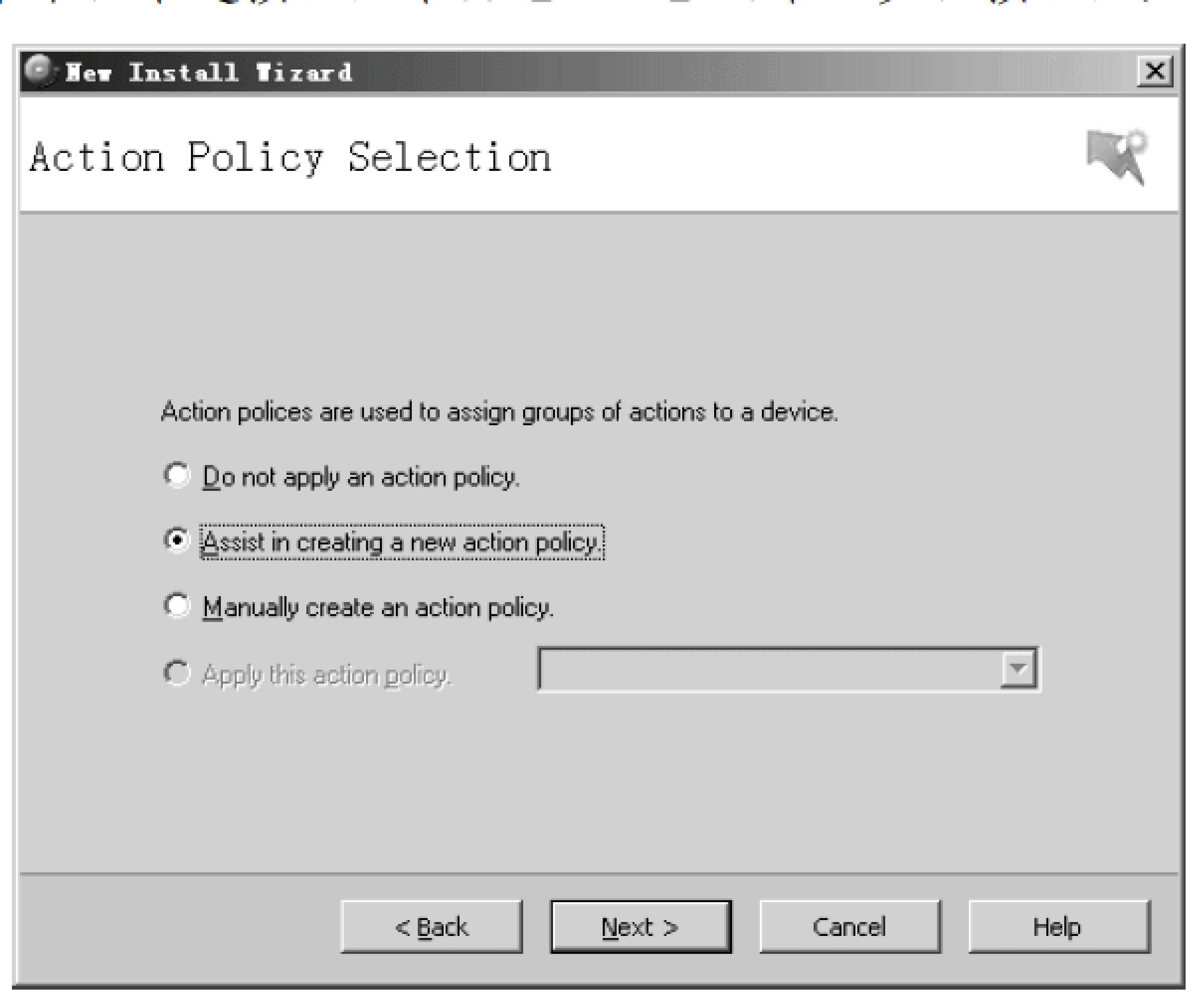


图 5-70

09 弹出【Action Strategies】（动作策略）对话框，共有三部分内容的设置，分别是：【If a device has been unresponsive for 5 minutes，notify me by】（如果一个设备丢失 5 分钟如何提醒我）、【If a device has been unresponsive for 20 minutes，notify me by】（如果一个设备丢失 20 分钟如何提醒我）、【When a device starts responding again,notify me by】（当一个设备重新连接时如何提醒我）。可以通过 E-mail 邮件、提示音、windows message 信息三种方式进行提醒，三项均选择 E-mail 邮件和提示音方式，单击【Next】（下一步）按钮，如图 5-71 所示。

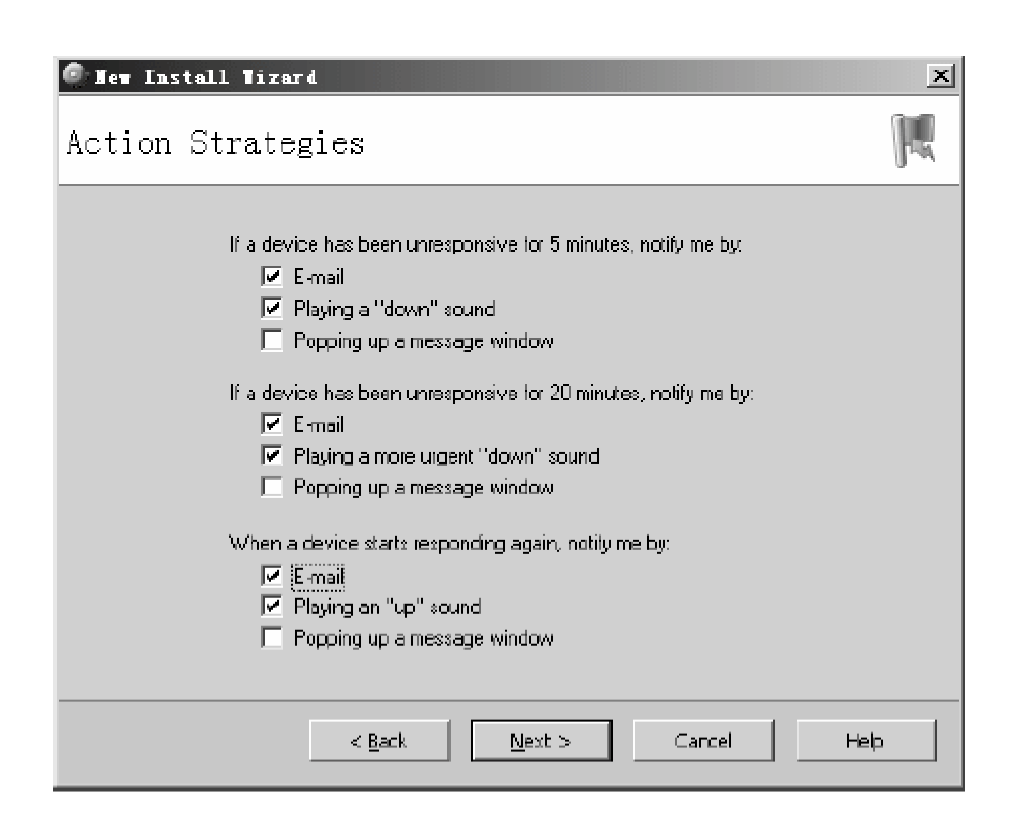


图 5-71

10 弹出【Internet E-mail Address】（邮箱地址设置）对话框，在【E-mail address】（邮件地址）文本框中输入有效的邮箱地址，在【Outgoing mail (SMTP) server】（向外发送邮件 SMTP 服务器）文本框中输入 SMTP 服务器地址，单击【Next】（下一步）按钮，如图 5-72 所示。

New Install Wizard
Internet E-mail Address
Enter the e-mail address you want the action e-mail sent to.
E-mail address: Example: someone@ipswitch.com
Test...
Outgoing mail (SMTP) server:
Port:
25
< Back
Next >
Cancel
Help

图 5-72

11 弹出【Action Policy Summary】（动作策略命名）对话框，在【Policy name】（策略名）文本框中输入策略名，本实例采用默认配置，单击【Next】（下一步）按钮，如图 5-73 所示。

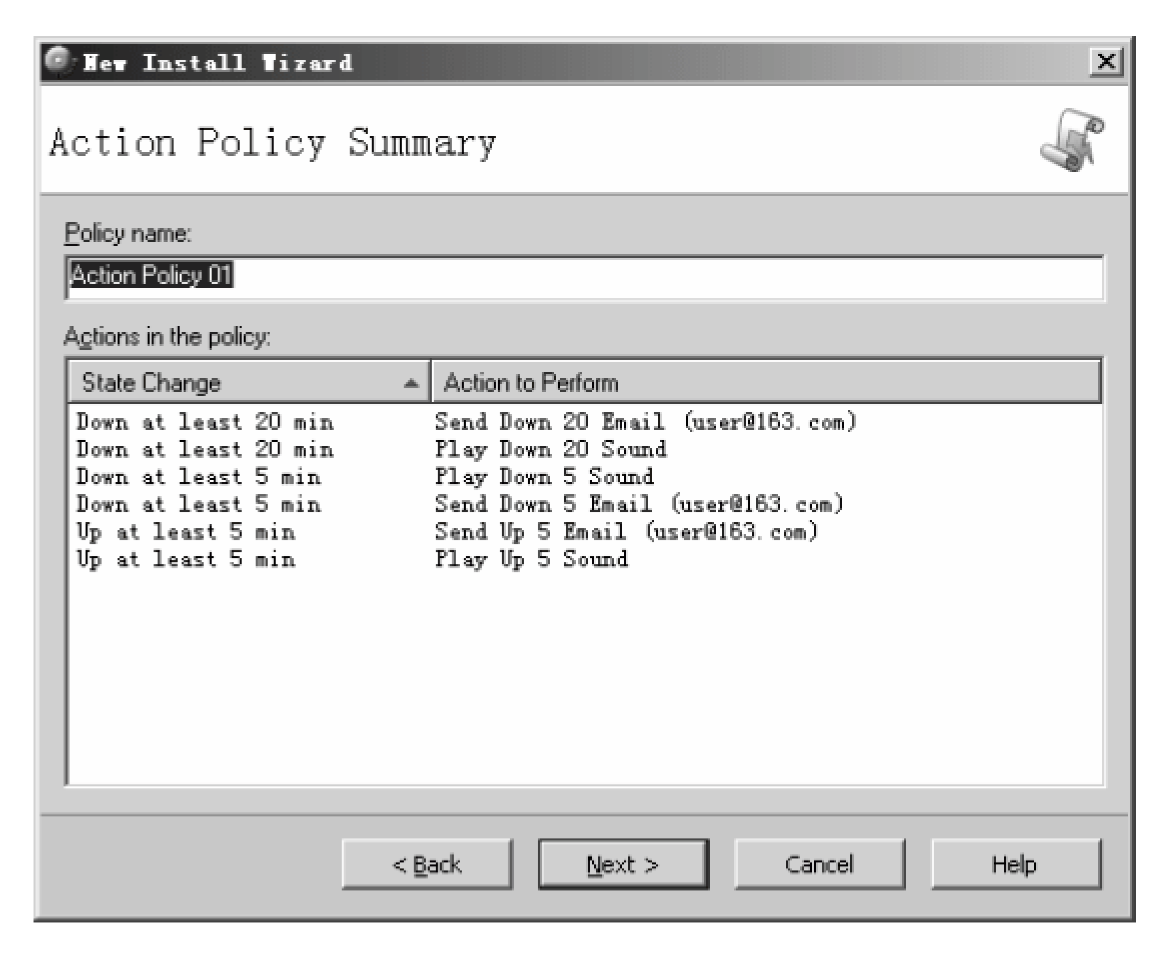


图 5-73

12 弹出【Finish】（完成）对话框，在其中显示出已配置的策略，单击【Finish】（完成）按钮，如图 5-74 所示。

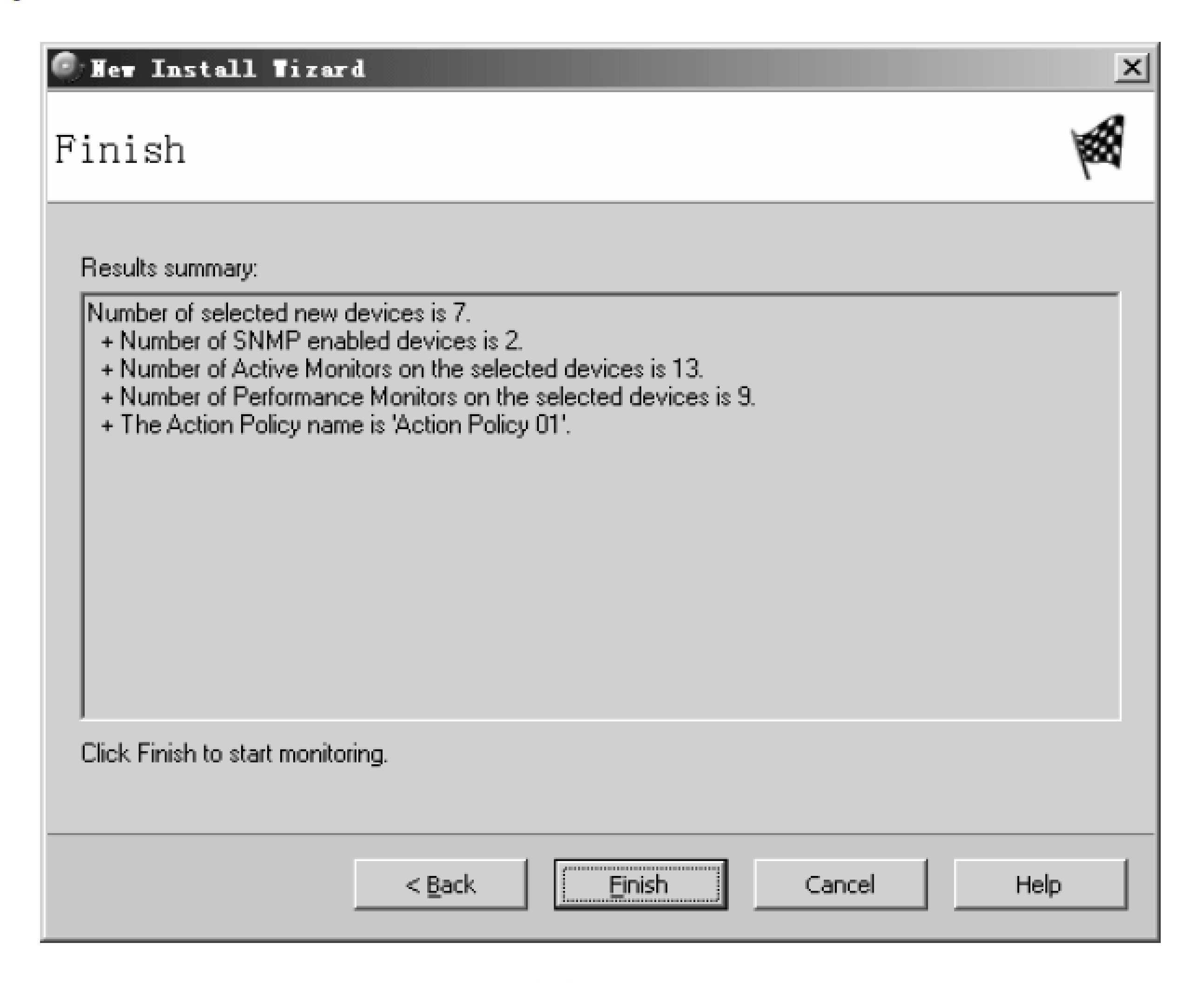


图 5-74

13 进入 WhatsUp Gold 程序主界面，窗口右侧显示了扫描结果，显示信息包括设备名、地址、设备类型等，如图 5-75 所示。

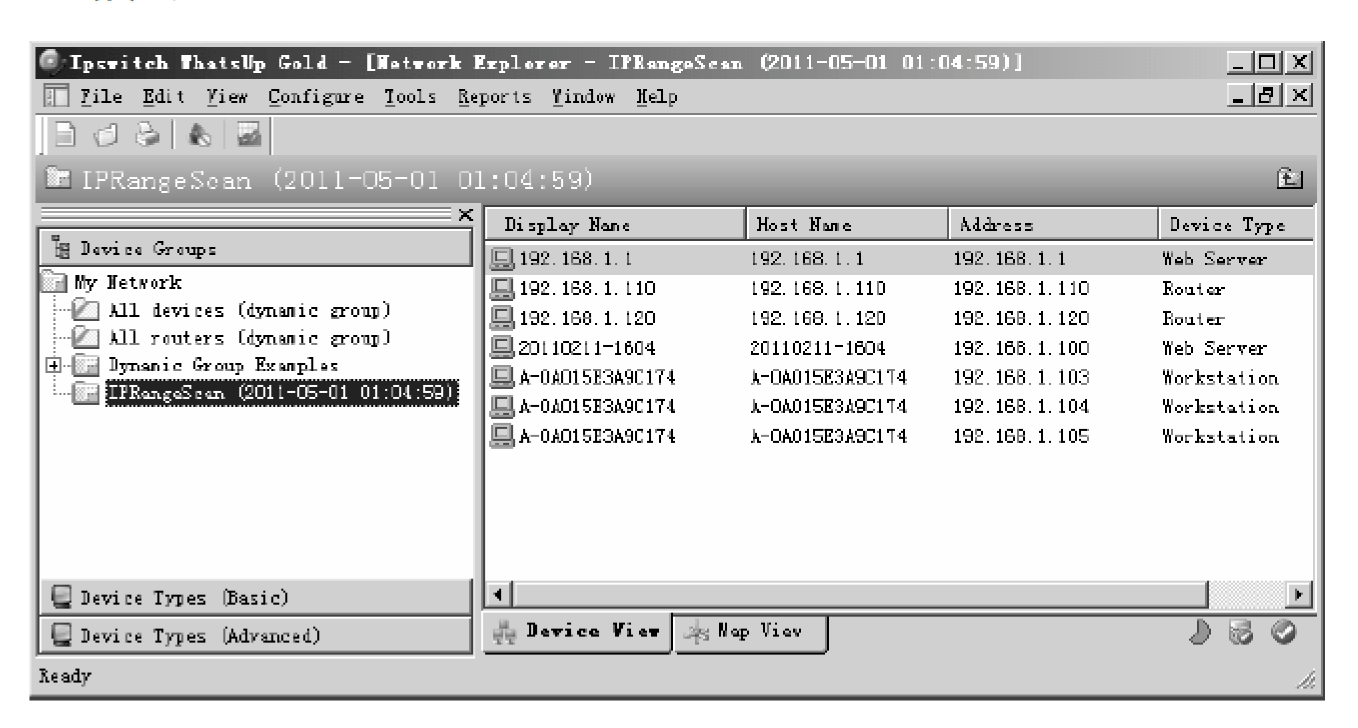


图 5-75

14 单击【Map View】（地图视图）选项卡，使用视图形式查看网络设备，如图 5-76 所示。

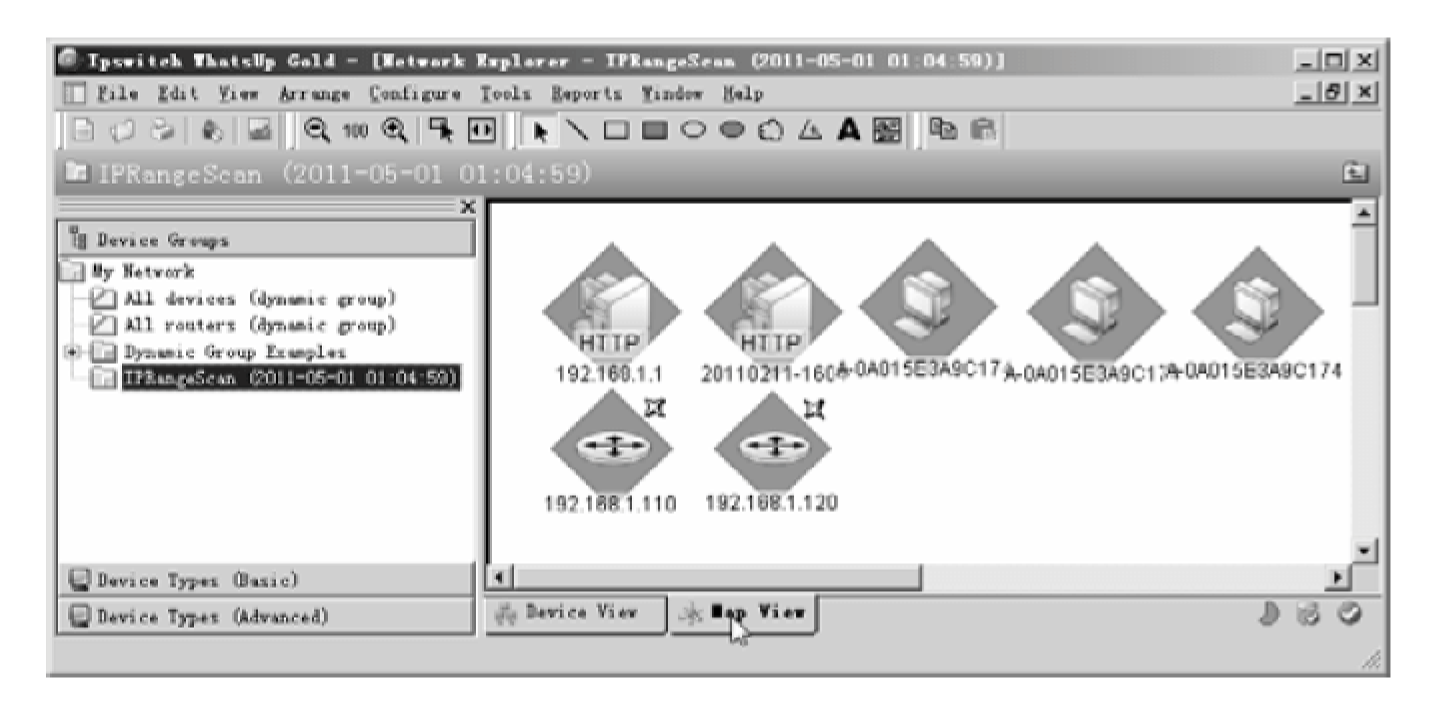


图 5-76

2. 拓展网络拓扑

第一次扫描往往不能获取网络内所有设备的信息，需要管理员手工添加未扫描到的设备，以完善网络拓扑结构。

添加新设备的具体操作步骤如下。

01 在 WhatsUp Gold 主界面左侧选择【Device Types (Basic)】（基本设备类型）选项列表，列表中显示了很多可添加的设备类型，如图 5-77 所示。

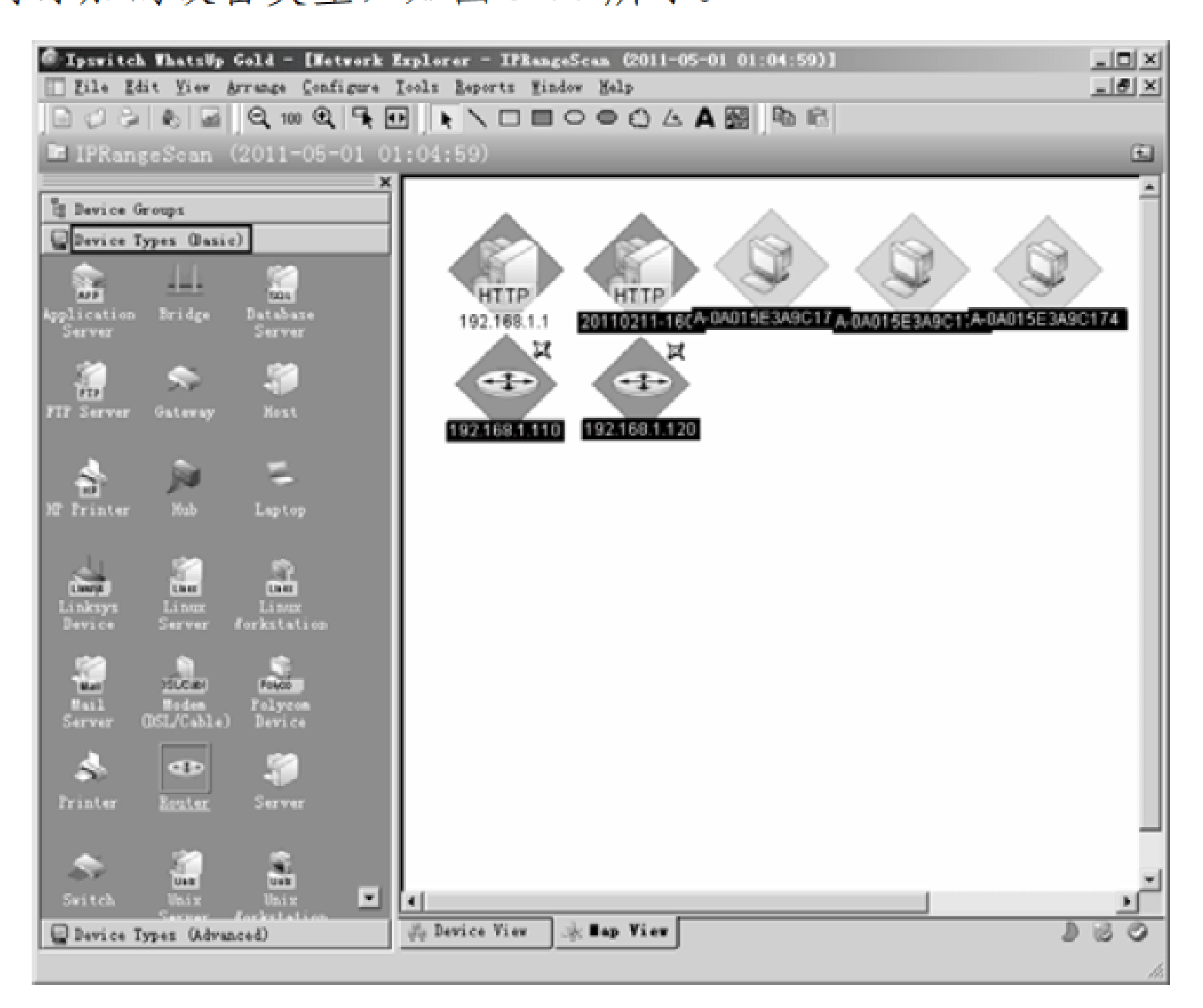


图 5-77

02 选择需要添加的设备类型，如【Router】（路由器），将其拖曳到右侧视图界面，如图 5-78 所示。

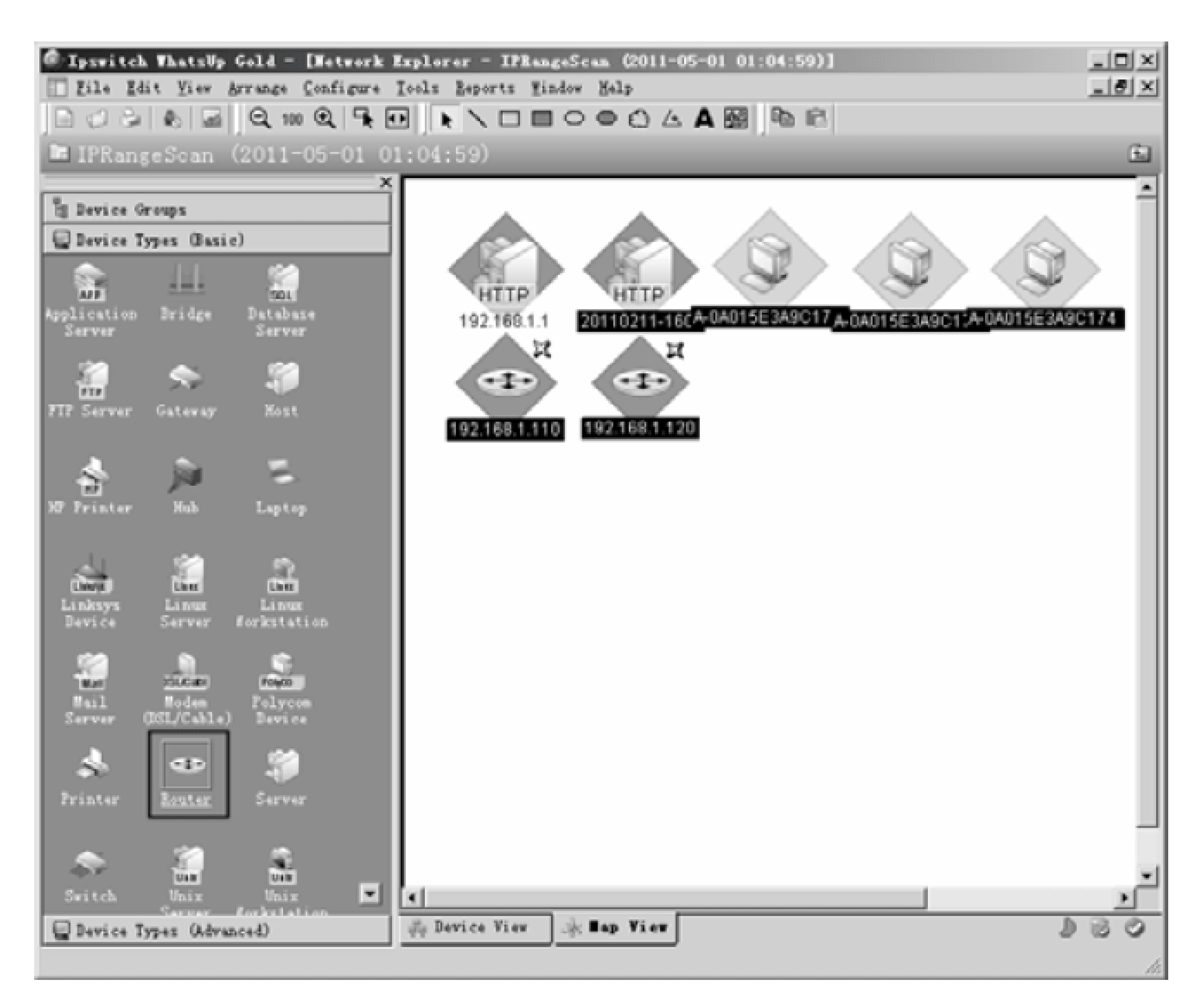


图 5-78

03 弹出【Add New Device】（添加新设备）对话框，在【IP address or host name of the new device】（新设备 IP 地址或主机名）文本框中输入要添加设备的 IP 地址或主机名，本实例采用“172.16.1.2”主机为例进行讲解，单击【Advanced】（高级）按钮，如图 5-79 所示。



图 5-79

04 在弹出的对话框中，选择需要获得目标设备的哪些信息，单击【OK】（确定）按钮，如图 5-80 所示。

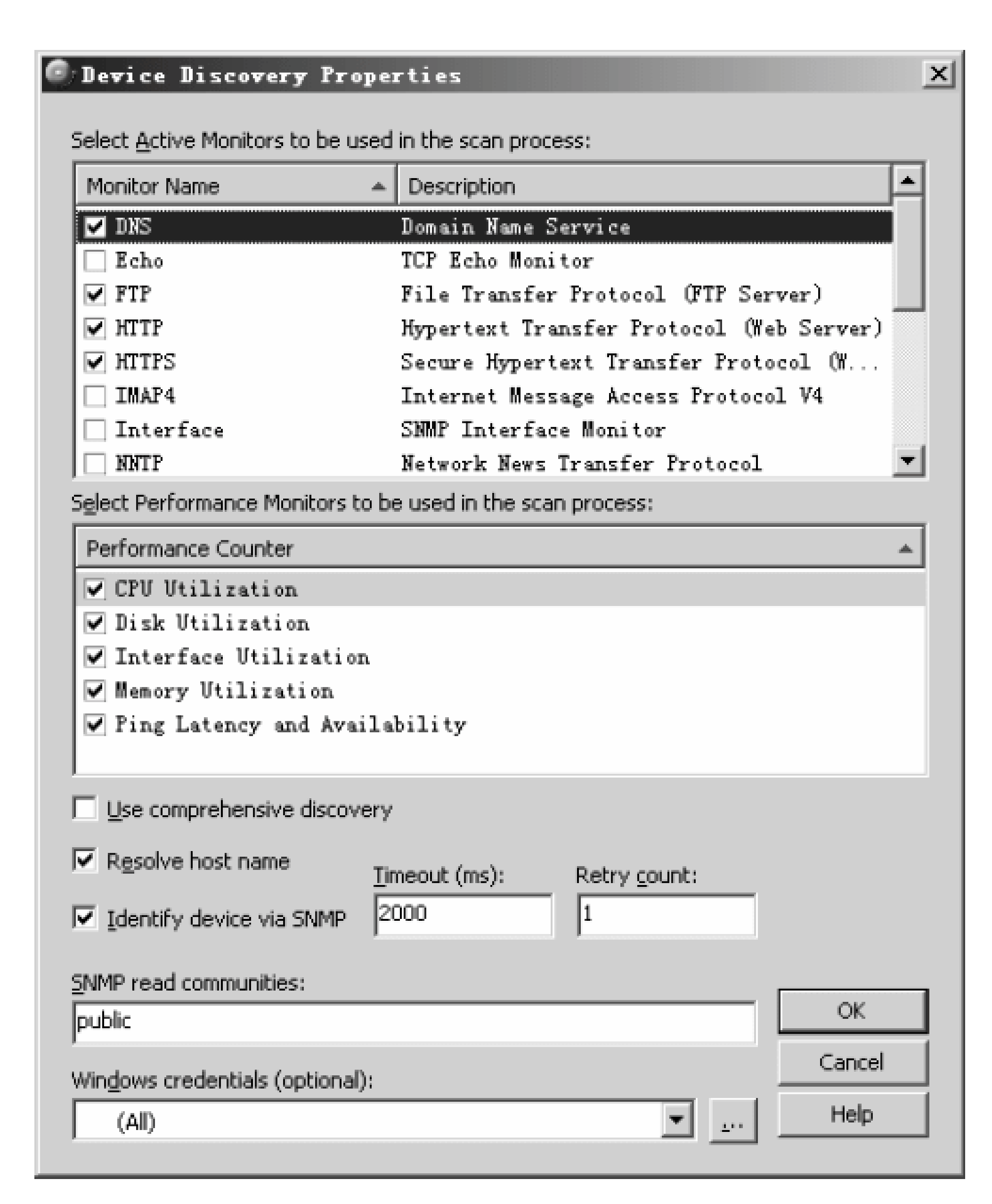


图 5-80

05 返回【Add New Device】（添加新设备）对话框，单击【OK】（确定）按钮，如图 5-81 所示。

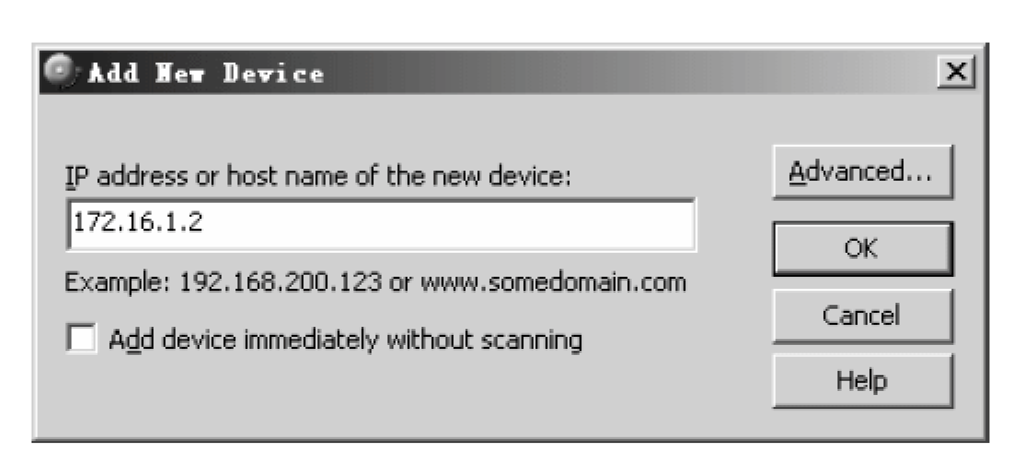


图 5-81

06 系统自动扫描主机信息，并显示扫描进度，如图 5-82 所示。

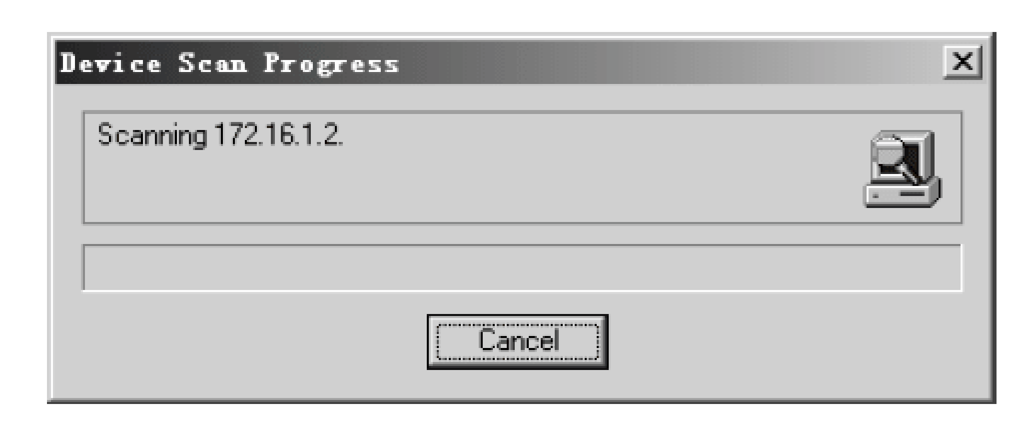


图 5-82

07 扫描结束，自动弹出设备 172.16.1.2 的基本信息配置界面，本实例采用默认配置，单击【OK】（确定）按钮，如图 5-83 所示。

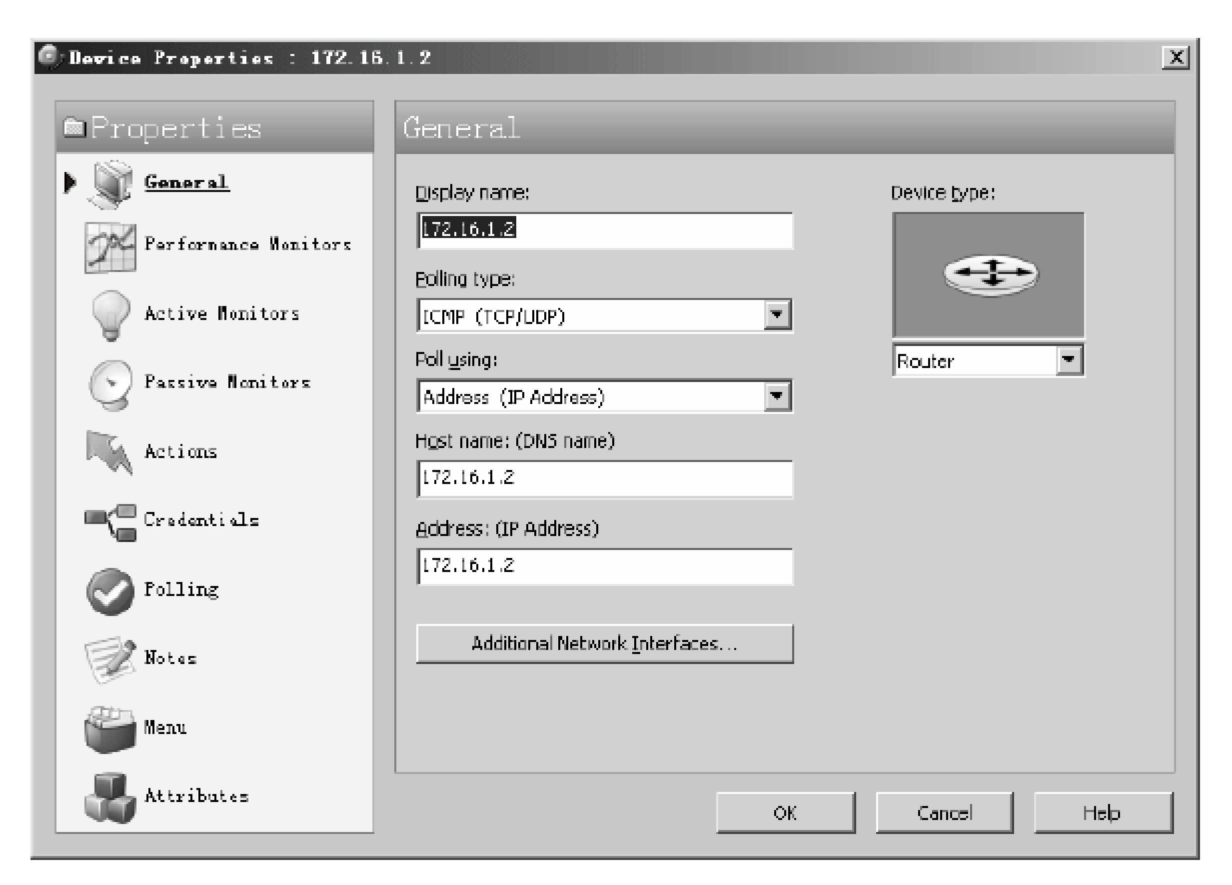


图 5-83

08 设备“172.16.1.2”添加成功，设备图标显示在右侧视图窗口，绿色表示设备可连通，如图 5-84 所示。

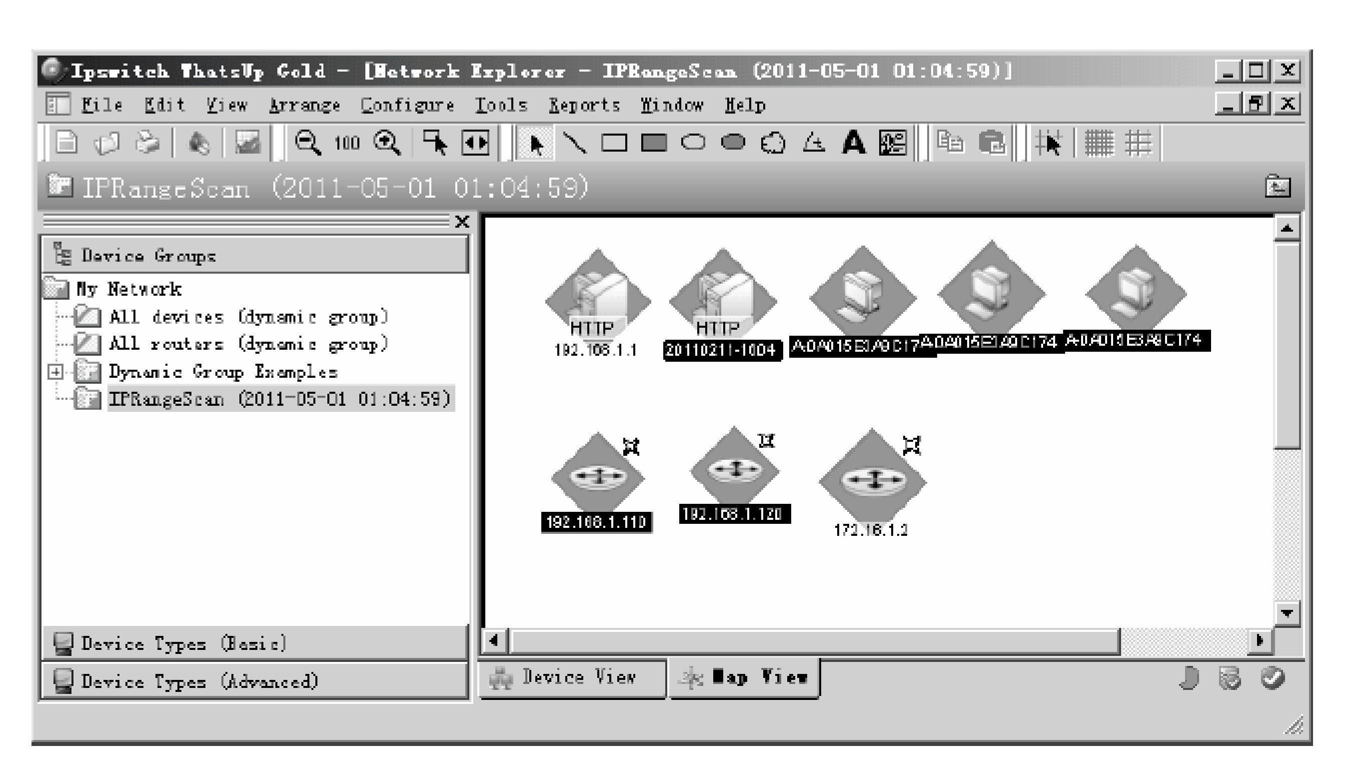


图 5-84

3. 调整设备链接关系，绘制网络拓扑图

设备添加成功后，只可以看到设备图标，但是无法看到所有设备的链接关系，不能直观的查看网络拓扑图，链接关系需要手工添加。

添加链接关系，绘制网络拓扑图的具体操作步骤如下。

01 右击图中某一网络设备，在弹出的快捷菜单中选择【Link】（链接）➢【Link to】（连

接到）菜单命令，如图 5-85 所示。

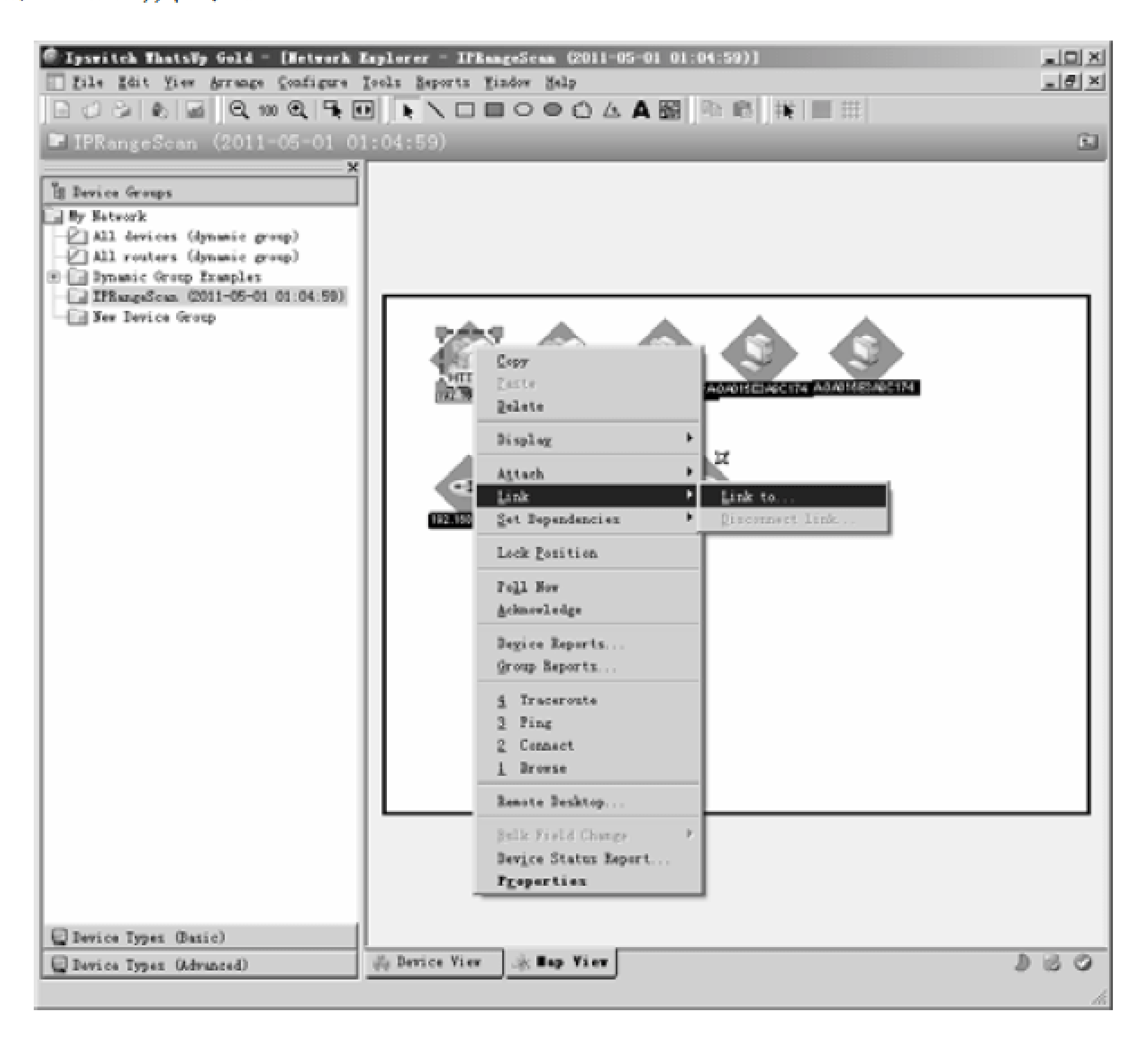


图 5-85

02 弹出【Select a Monitor to Link】（挑选一种方式连接）对话框，选择适当的测试连通方式，本实例采用“Ping”方式，单击【OK】（确定）按钮，如图 5-86 所示。

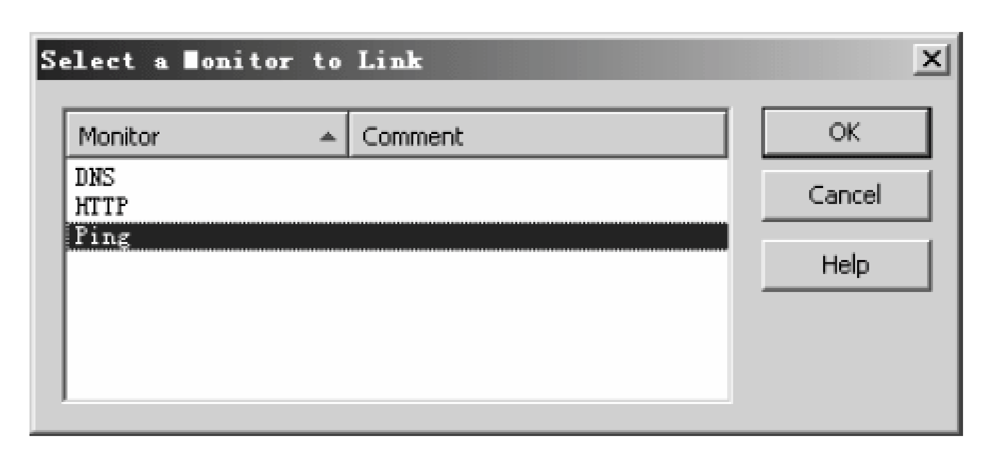


图 5-86

03 鼠标指针显示带有“+”号的短线，单击要连接的设备，如图 5-87 所示。

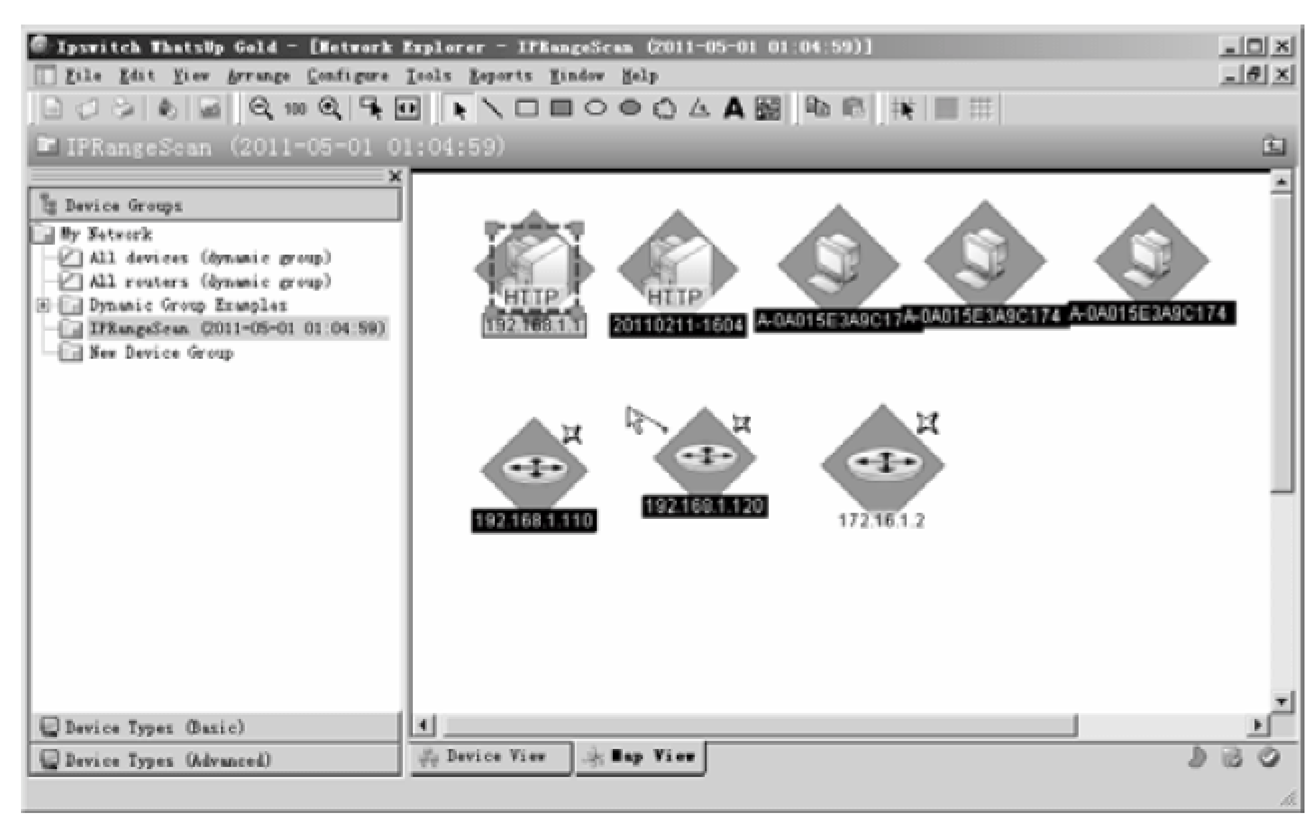


图 5-87

04 选择的两个设备会通过 “Ping” 命令测试连接状态，链接关系建立成功后如图 5-88 所示。

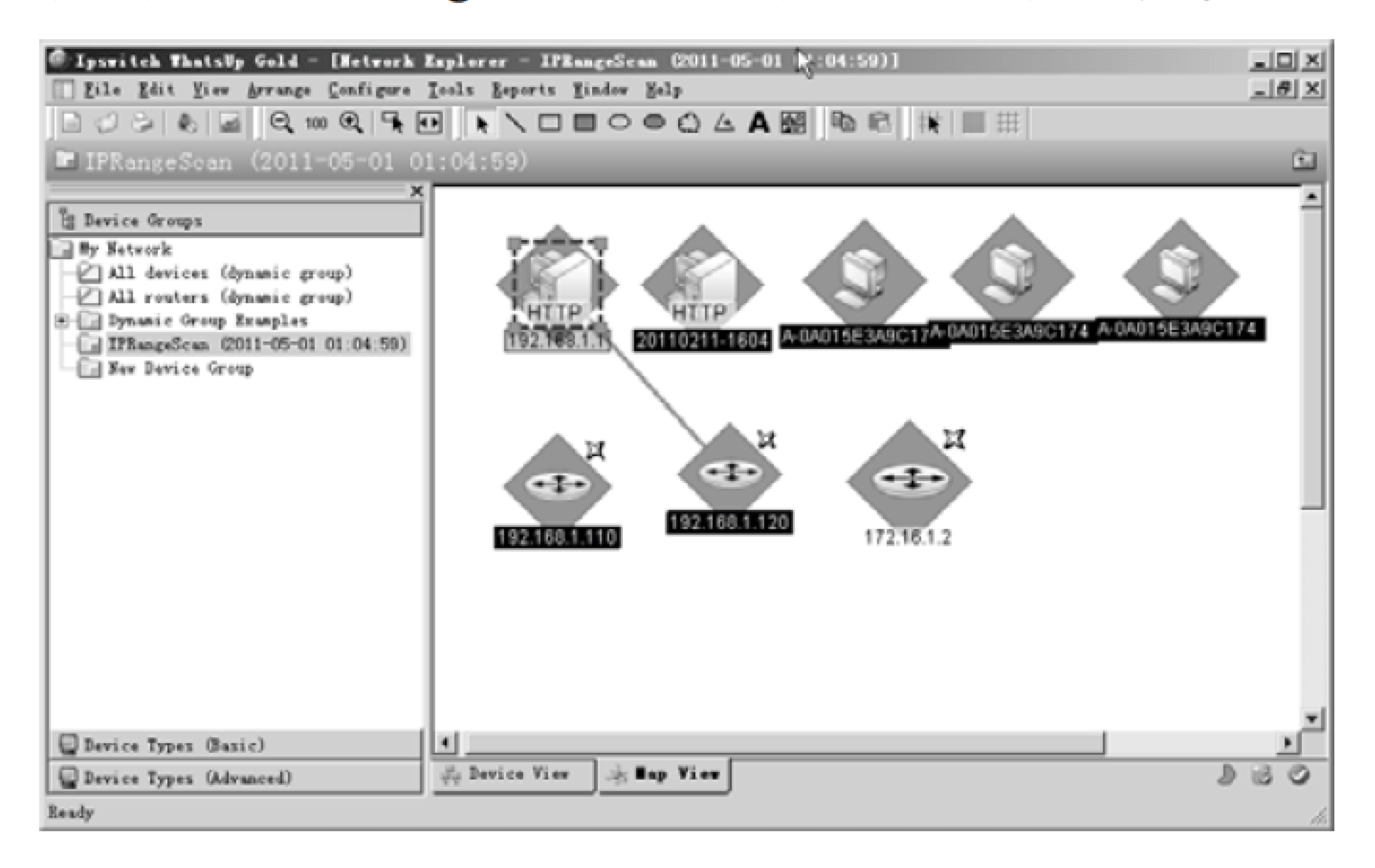


图 5-88

05 根据网络设备链接状况，添加所有设备及链接关系，形成最终的网络拓扑图，如图 5-89 所示。

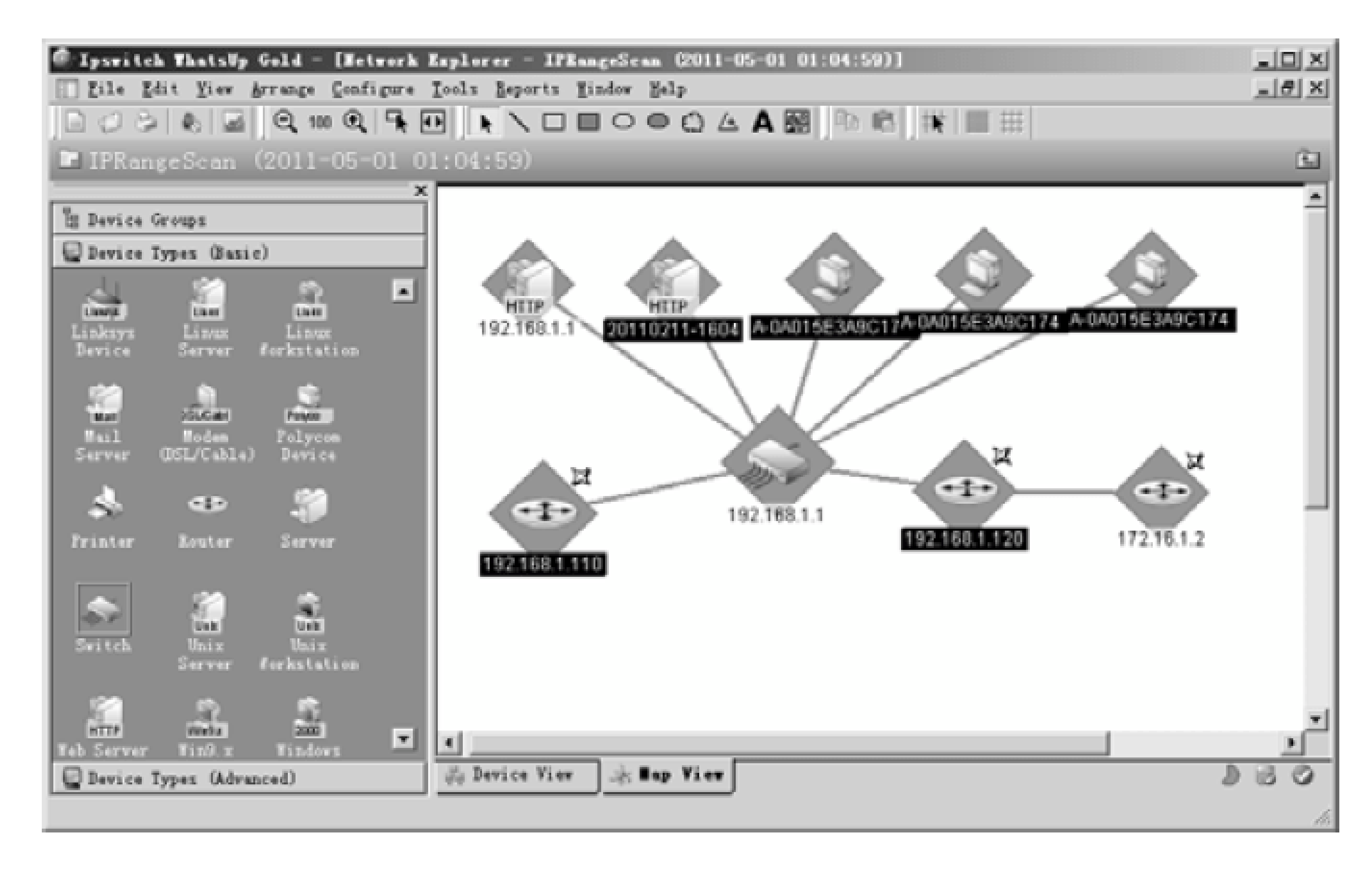


图 5-89

5.3.3 查看网络设备信息

使用 WhatsUp Gold 可以通过网页形式查看设备的信息，具体操作步骤如下。

01 右击需要查看的设备图标，在弹出的快捷菜单中选择【Device Reports】（设备报告）菜单命令，如图 5-90 所示。

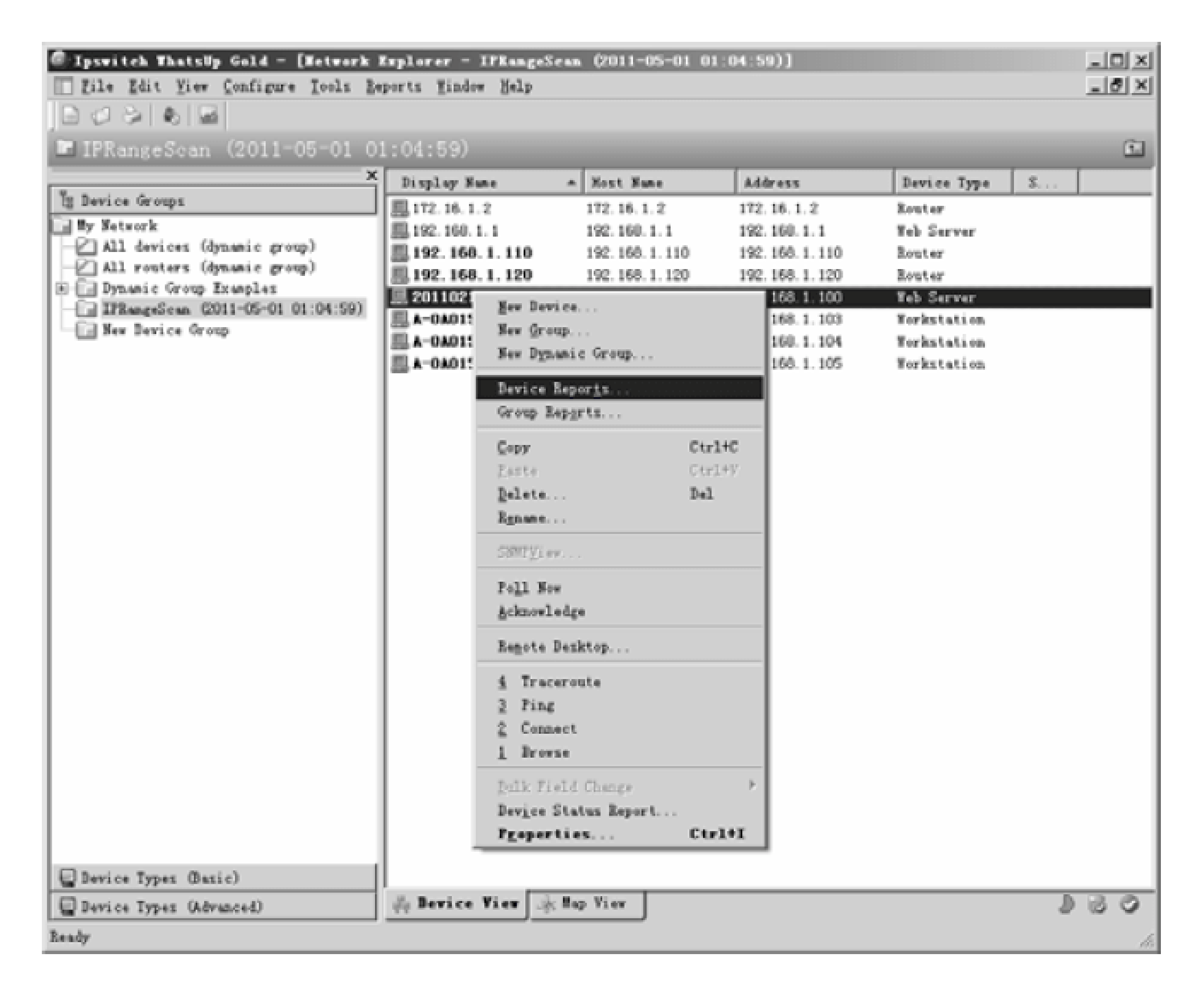


图 5-90

02 打开 WhatsUp Gold 网页登陆页面，在【User Name】（用户名）文本框中输入登陆用户名，在【Password】（密码）文本框中输入登录密码，用户名及密码默认为“admin”，单击【Login】（登录）按钮，如图 5-91 所示。



图 5-91

03 进入设备报告查看页面，单击页面内的选项可以查看到各种相关信息，如图 5-92 所示。

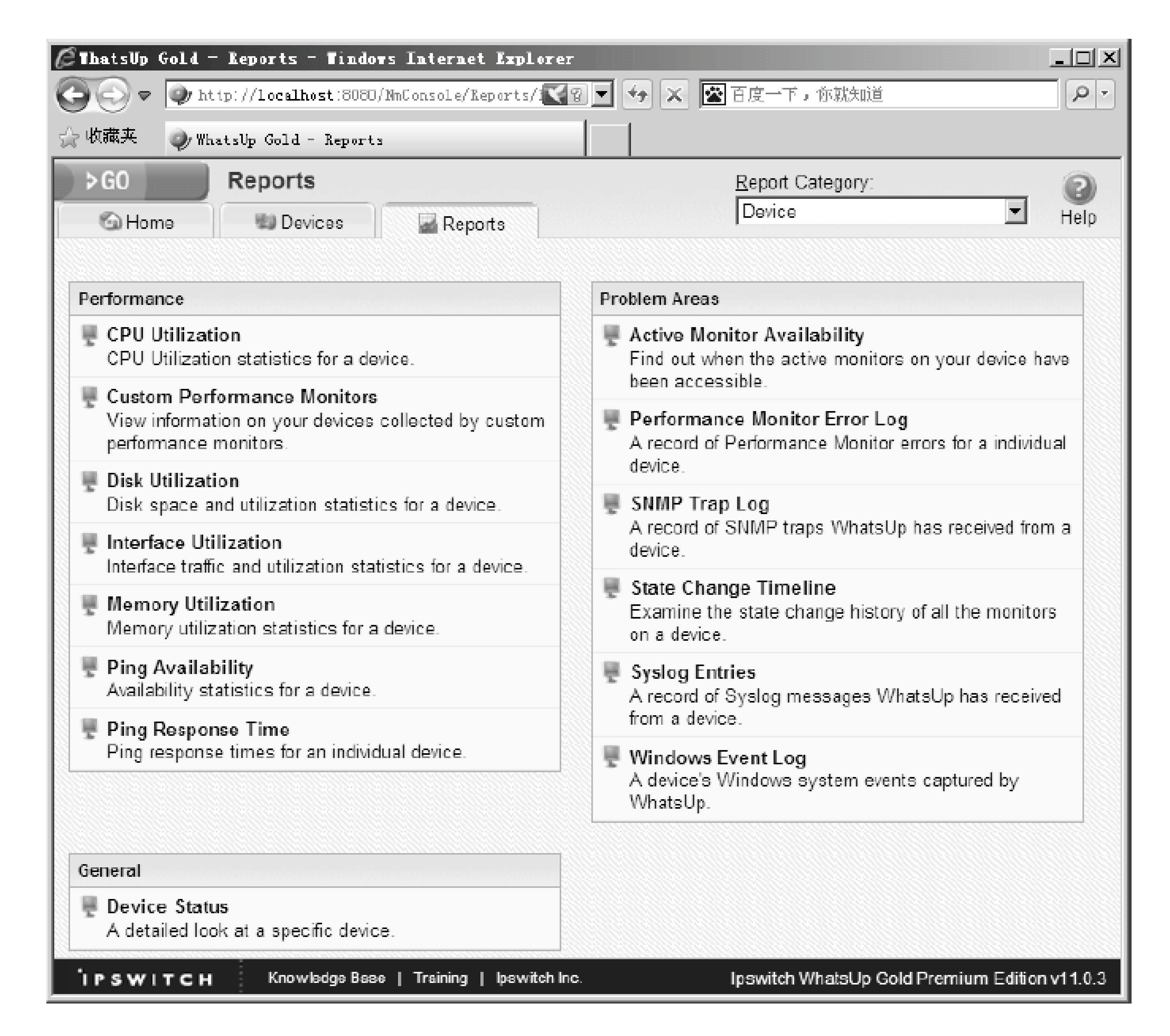


图 5-92

04 打开【Devices】（设备）选项卡，在右侧窗口中双击需要查看信息的设备，本实例使用“192.168.1.120”为例进行讲解，如图 5-93 所示。

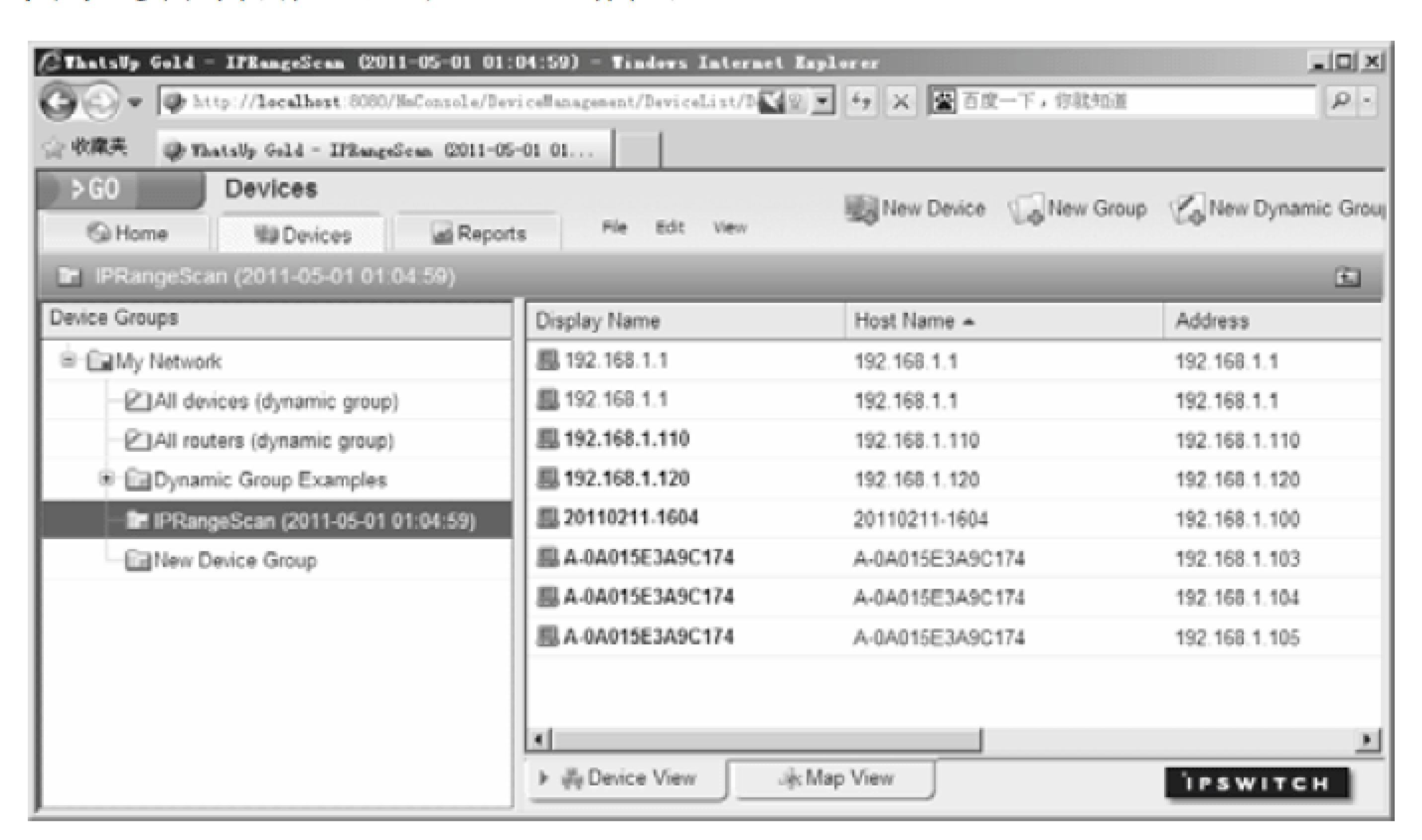


图 5-93

05 进入设备“192.168.1.120”的信息统计界面，通过界面可以获得设备的性能列表、基本信息、日志信息、SNMP 协议信息等，如图 5-94 所示。

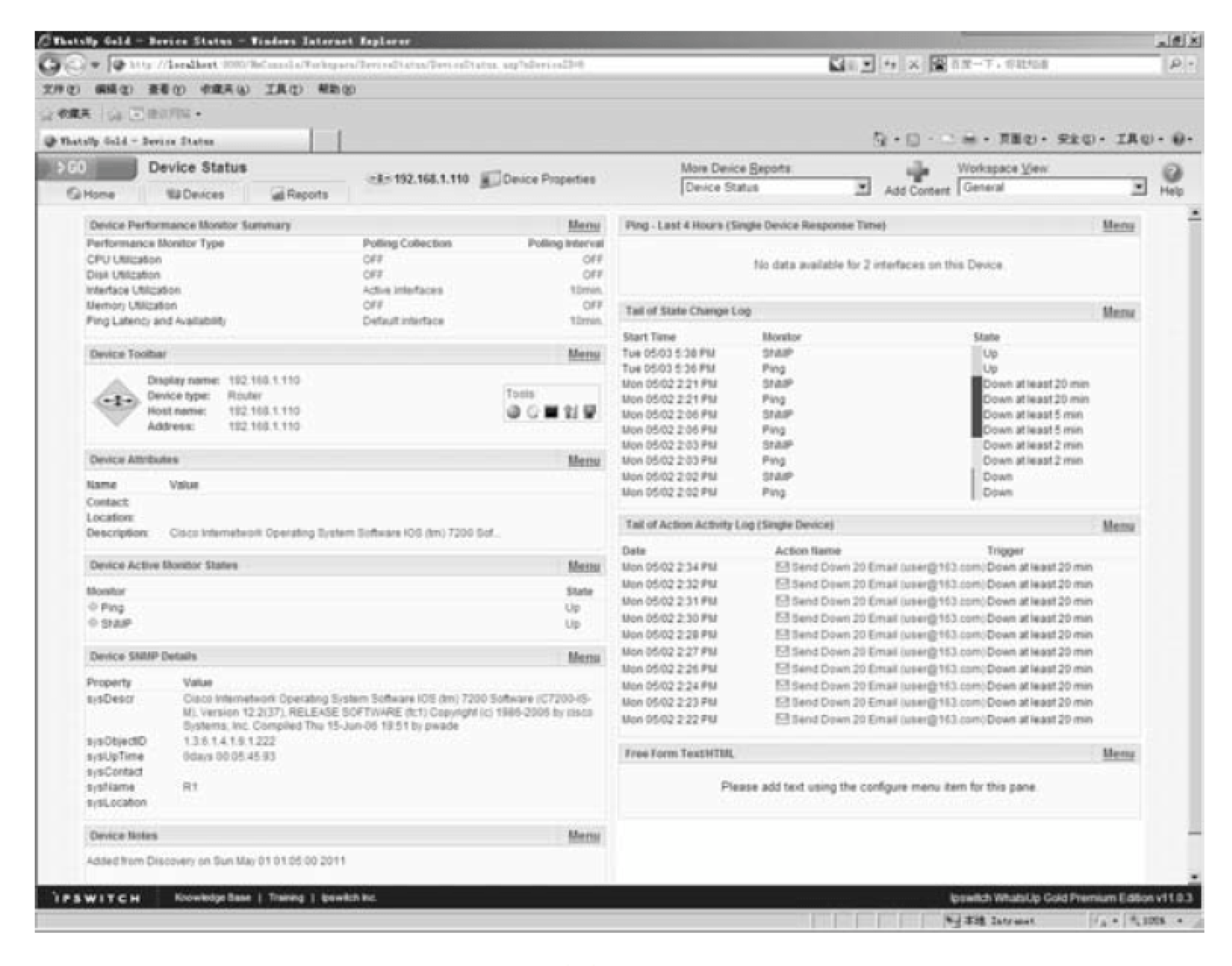


图 5-94

5.3.4 网络故障发现与修复

网络运营中会出现很多链接问题，通过 WhatsUp Gold 可以清晰地看出故障问题，具体显示效果如下。

（1）网络设备刚断开时，设备图标形状和颜色变化如图 5-95 所示。

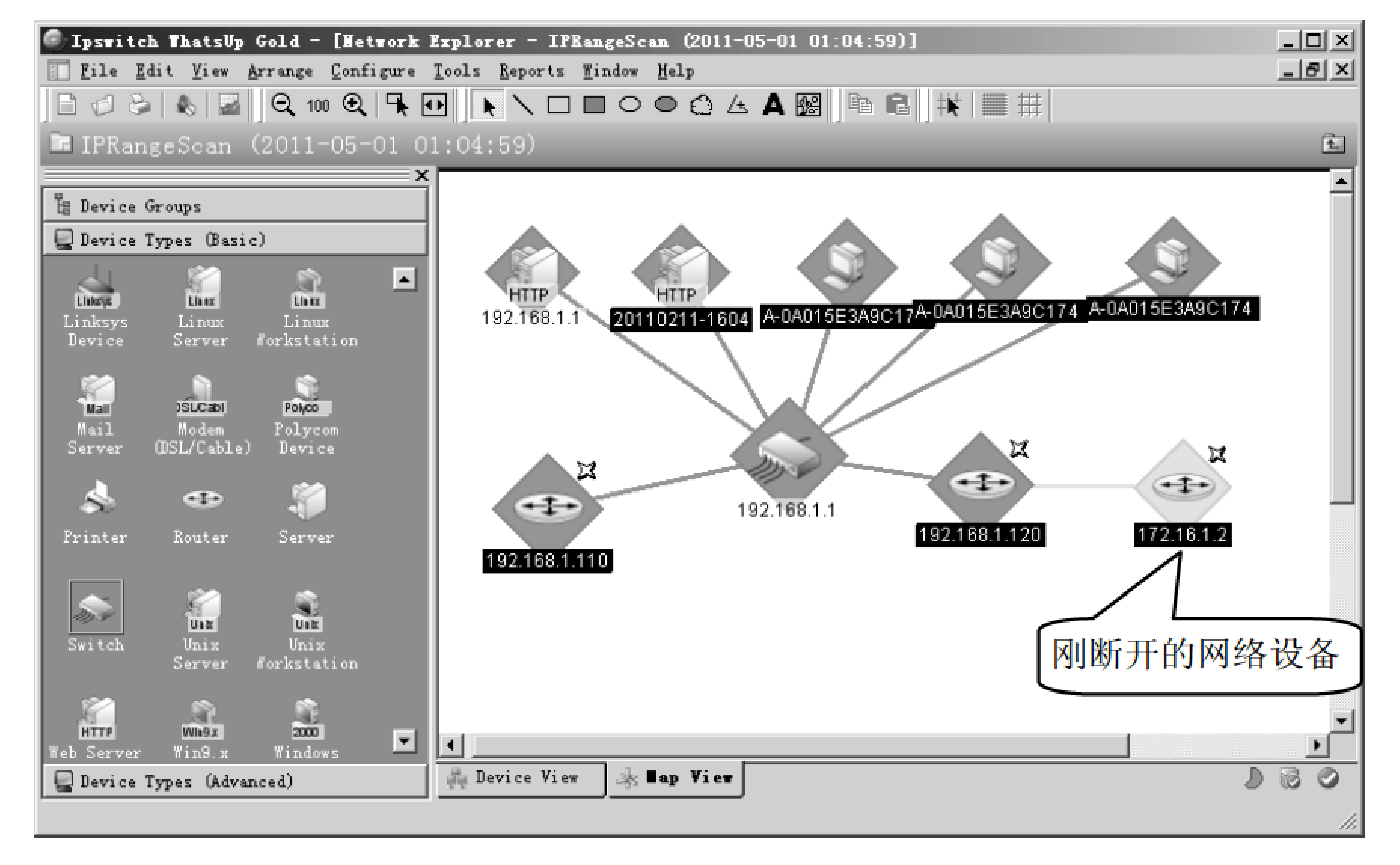


图 5-95

（2）网络设备断开 2 分钟后，设备图标形状和颜色变化如图 5-96 所示。

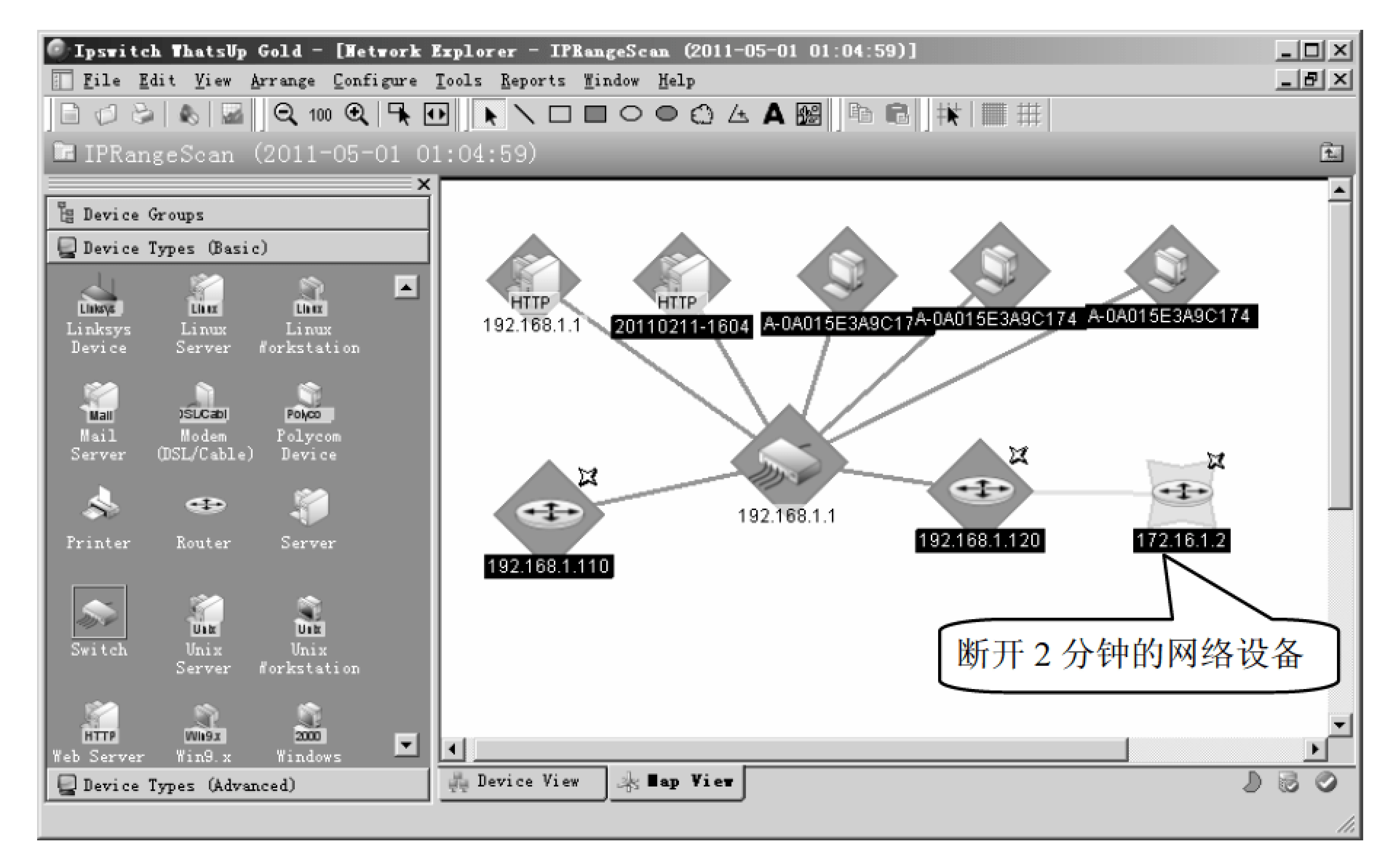


图 5-96

（3）网络设备断开 5 分钟后，设备图标形状和颜色变化如图 5-97 所示。

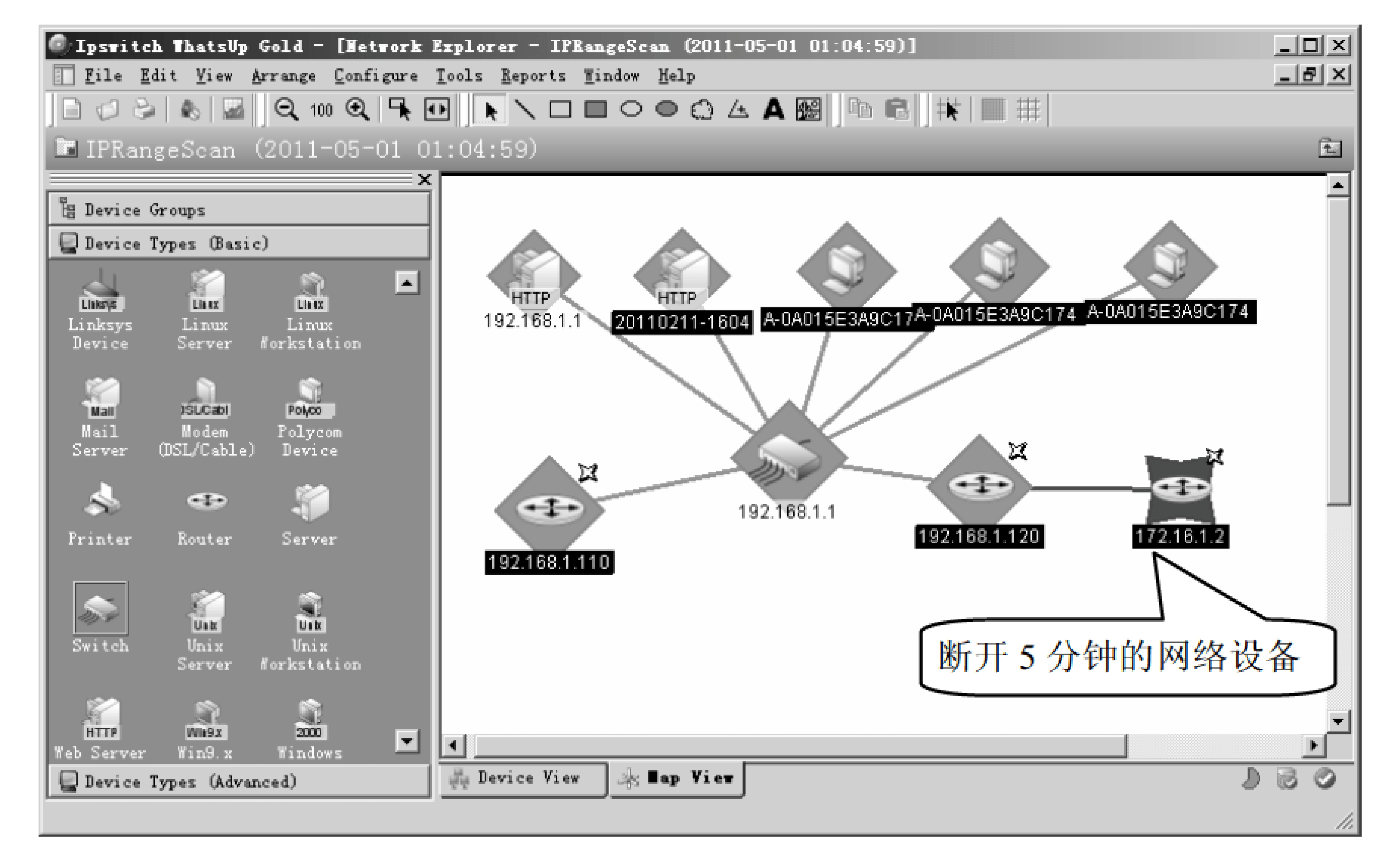


图 5-97

（4）网络设备断开 15 分钟后，设备图标形状和颜色变化如图 5-98 所示。

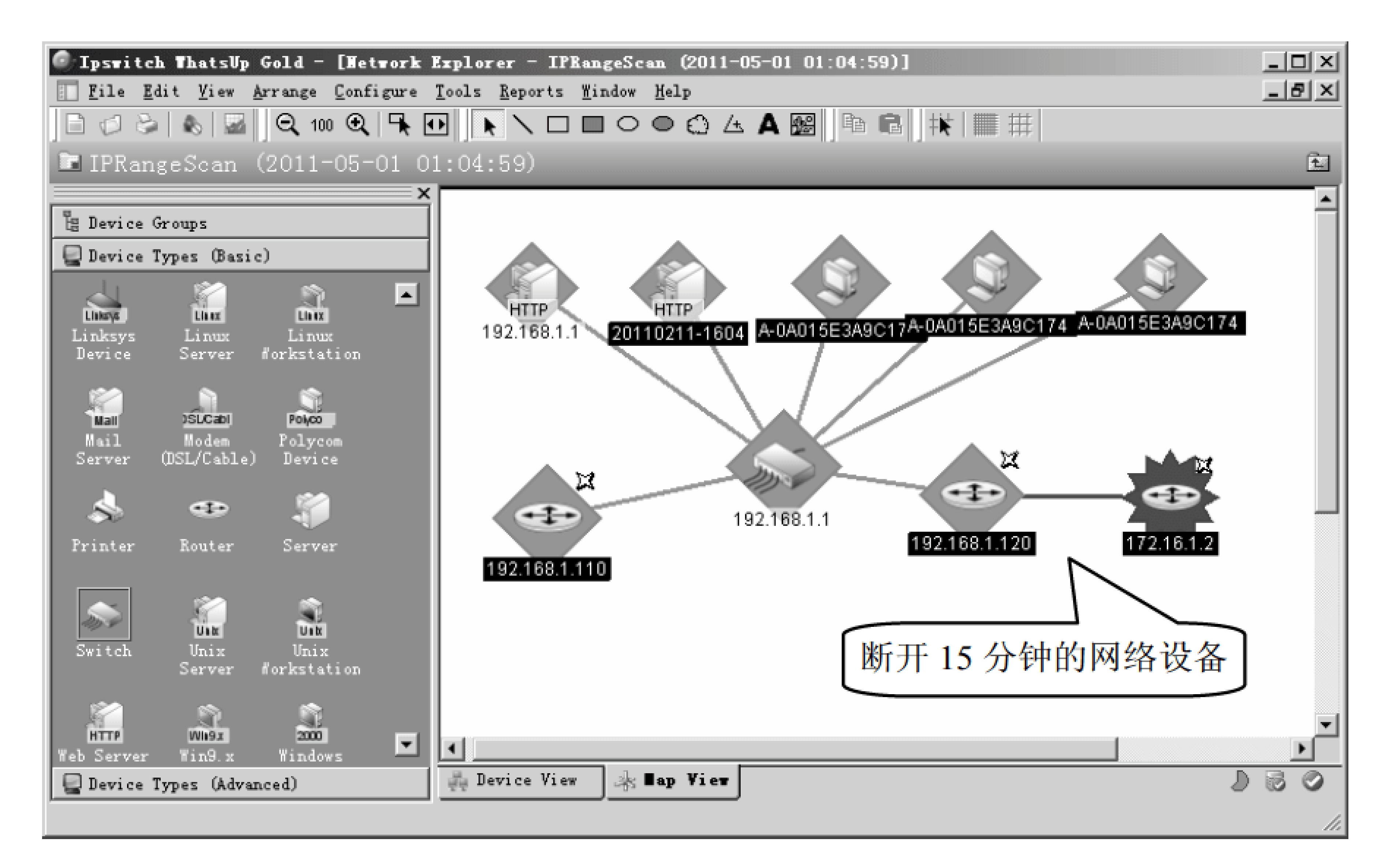


图 5-98

在设备图标背景变化的同时，服务器会随之发出提示音，并向提前设定好的邮箱地址发送邮件。这类问题一般是网络线缆问题或网络设备问题，需要网络管理员排查检修。

网络故障排除的具体思路如下。

01 通过其他工具测试是否能与该设备通信，同时可以采用多种协议测试。通过测试结果判断故障问题，如果部分协议可通信，可以考虑是否在网络中添加了访问策略。

02 通过其他方法依然无法连通时，要先考虑断开设备是否当机，或做了配置调整，导致网络不可达。管理员可以到设备附近，调试配置设备。通过终端连接测试后设备运行没有问题，可排除该故障。

03 网线在使用时也可能被损坏，可以使用测试工具对网线的连通做测试。

04 网线测试没有问题，也可能是网线接口故障，可以更换接口再做测试。

以上步骤只是通用步骤，可能在网络中出现特殊故障原因，管理员可以根据实际情况进行排查。

5.4 专家答疑

（1）使用网络管理平台监控、查看设备时，为什么不能获得设备的详细信息及性能？

答：可以从两个方面考虑出现这一现象的原因。其一，网络设备连接是否正常，可以通过网络测试工具，测试网络连接状态；其二，获取详细信息需要有网络管理协议的支持，可以查看被管设备是否安装、开启了 SNMP 网络管理协议，或者是 SNMP 协议使用的团体名是否一致，默认团体名为 public。

（2）使用 Spiceworks 网络管理平台监控网络时，网页内的部分信息无法显示，并且经常弹出

如图 5-99 所示提示框。

Your Browser is Incompatible with Spiceworks

Either you have JavaScript, cookies, or Stylesheets (CSS) turned off or you are using a browser without the features required to use Spiceworks.

Spiceworks is compatible with modern browsers, and requires JavaScript, Cookies, and Stylesheets (CSS) to function correctly.

If your browser meets these requirements and you are still having issues, please send an e-mail to support@spiceworks.com with an explanation of the problem.

图 5-99

答：出现这类问题的主要原因是，在使用 Spiceworks 网络管理平台查看信息时，网页中要显示动态信息，如果系统没有安装 JavaScript 环境或没有 CSS 文件，动态网页信息无法显示。所以在使用 Spiceworks 软件前，一定要先安装好动态网页浏览环境。

第 6 章　服务器的监控与管理

服务器作为网络中最重要的设备之一，是网络管理中不容忽视的部分。服务器性能的好坏直接影响到服务器的工作效率，对整个企业的业务运作有很大影响。如何让服务器稳定、可靠地工作，成为了不少网络管理员必做的工作之一。同时，如何高效、准确地进行服务器管理，也是管理员所关注的问题。

6.1　服务器管理需求分析

在实施服务器管理之前，首先要了解什么环境下会用到服务器远程管理技术，并且要明确对服务器进行哪些管理操作。

1. 什么情况需要使用服务器远程监控管理技术

大多数的服务器都放置在机房里，不需要管理员到设备面前操作。一般都是采用远程桌面连接的方式，但是这种方式安全性较低，而且只能实现对远程设备的控制，却无法直观地监控其性能、工作状态。

有些企业服务器是整个公司业务运作的支柱，一旦服务器性能出现故障很容易造成损失。必须要有能实时的为管理员提供服务器性能状态信息的程序，这时就需要远程服务器监控程序了。这些专业的服务器监控程序不但可以实现服务器的远程配置，同时还可以实现服务器性能状态的实时分析，并以图表、报告的形式予以显示。除此之外，远程服务器监控程序比远程桌面连接的安全性高很多，有些程序需要管理员使用指定的端口、口令、主机 IP 或管理端程序才可以实现连接。

2. 需要对服务器进行哪些方面的监控与管理

通过远程服务器监控程序，需要对服务器做以下几项工作。

- 对服务器的系统配置、软件程序具有调试管理权限。
- 能够实时的监控系统的网络访问流量，并能对流量进行简单的分析。
- 能够动态的反应系统及服务器当前的运行状态。
- 能够实时的查看 CPU、内存、硬盘等硬件的性能状态。
- 能够获得完善的系统日志。

6.2　服务器性能指标分析

通过远程监控管理，会涉及到很多表示服务器性能的参数指标，在进行管理前必须要理解这些性能指标的意义。性能是决定服务器可用性、稳定性的决定因素，任何一台服务器，最值得关注的就是其性能。

6.2.1　服务器性能指标

服务器的性能指标可以根据应用不同进行分类，经常用到的有系统通用性能指标、Web 服务器指标、数据库服务器性能指标。下面分别进行介绍。

1. 通用性能指标

大多数服务器除去服务，使用最多的性能指标有以下三种。

（1）Processor Time（CPU 占用率）：用于显示 CPU 的性能，一般 CPU 的占用率不应该长期超过 70%~80%，通过图表查看 CPU 性能长期超过限定值时，要对系统进行分析，确定是需要升级服务器，还是有不当配置或恶意程序需要处理。

（2）Memory Available Mbyte（可用内存数）：用于显示内存性能，内存空闲数量影响着整个系统服务的运行，虽然可以增加虚拟内存，但是物理内存也不能长期处于被大量占用的状态。

（3）Physicsdisk Time（物理磁盘读写时间情况）：磁盘的读写速度对服务器的运行、访问影响很大，当磁盘读写速度明显下降时要考虑是否磁盘有坏道，要在故障发生之前及时修复或更新磁盘，以避免磁盘彻底损坏，数据丢失。

2. Web 服务器指标

Web 服务器是使用最多的服务器，它需要关注的性能指标有以下几种。

（1）Requests Per Second（平均每秒钟响应次数）：统计一个时间段内的平均请求次数，通过统计可以比较是否在某些时间段出现大量响应，以判断是否为非法访问。

（2）Successful Requests（成功的请求）：查看一个时间段内成功请求的数量，和服务器本身所能承受的请求数进行比较，确定是否需要调整配置或升级服务器。

（3）Failed Requests（失败的请求）：统计一段时间内失败的请求数，用以判断服务器是否有访问故障或者是否有网络攻击存在。

（4）Successful Hits（成功的点击次数）：在网络访问时，虽然网页可以连接到，但是只有部分连接可以点击成功，有些却不能成功，本性能参数统计的是成功点击数。

（5）Failed Hits（失败的点击次数）：统计单位时间内失败的点击数，如果统计量过大可以考虑是否服务器的个别连接出现了异常。

（6）Hits Per Second（每秒点击次数）：单位时间内的点击数。

（7）Successful Hits Per Second（每秒成功的点击次数）：单位时间内成功的点击数。

（8）Failed Hits Per Second（每秒失败的点击次数）：单位时间内失败的点击数。可用于发现

服务故障。

3. 数据库服务器性能指标

除了 Web 服务之外，企业内的重要数据都需要专业的数据库服务器进行管理，所以数据库服务器的性能也是至关重要的，它需要关注的性能指标有以下几种。

（1）User Connections（用户连接数）：数据库并发连接数量统计，可以和数据库本身允许的最大连接数比较，判断是否到达上限。

（2）Number of deadlocks（数据库死锁数）：对数据库错误运行或访问出现死锁情况的反映，用于发现故障。

6.2.2 性能测试的目的

对服务器进行性能检测主要是为了验证软件程序或系统是否能够达到用户提出的性能指标，以此来判断软件程序或系统中是否存在性能瓶颈或服务故障，进而实施软件、系统优化，达到系统服务稳定运行的目的。

细致划分，性能测试的目的包括以下几个方面。

1. 评估系统的工作能力

通过测试，可以得到系统的负荷和响应时间数据，通过这些和服务架设要求进行比较，判断系统是否能满足当前架设服务的需求，并做出调整、升级。

2. 查找服务架设体系中的问题

通过性能数据，可以查找系统服务的瓶颈，并加以改善，使系统服务达到性能的全面发挥。同时还可以对错误信息进行分析，找出系统程序中隐含的问题加以调整。

3. 验证稳定性和可靠性

稳定性和可靠性是每一个服务器最先要考虑的问题，只有稳定可靠的运行才可能实现其服务的意义。通过获取的性能信息，可以对此做出判断，并能判断出影响系统稳定性及可靠性的因素。

6.3 服务器远程控制工具介绍

实现服务器远程管理的方法有很多，最常见的有 Telnet、ssh、vnc、远程桌面等技术。除此之外还有一些专门的服务器远程控制工具，如 RemotelyAnywhere、pcAnywhere 等。下面对以上几种技术、工具进行详细介绍。

6.3.1 Telnet

Telnet 是远程服务器管理中使用最普遍的技术，它属于 TCP/IP 协议族，是 Internet 远程登陆服务的标准协议和主要方式。在本地计算机上运行 Telnet 程序，可以连接到远程服务器，并通过终端

命令实现对远程主机的控制。

Telnet 技术主要是通过 DOS 命令实现管理控制。通过 DOS 命令管理有很多的优点，首先在控制端与被控制端不会有图形信息传输，提高了信息的传输效率；其次使用 DOS 命令可以实现很多强大的控制功能，提高了远程控制效率。想要使用 Telnet 技术，管理员首先要熟悉常用的 DOS 命令，但是 DOS 命令繁多，不易记忆，操作不够直观，让很多管理员望而却步。所以建议将 Telnet 当做一种辅助管理技术来使用。

想要让终端主机控制远程服务器，需要先建立 Telnet 连接。在建立连接时，要求两端的 Telnet 服务均处于开启状态。

开启 Telnet 服务的具体操作步骤如下。

01 选择【开始】>【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“services.msc”命令，如图 6-1 所示。



图 6-1

02 弹出【服务】窗口，在右侧区域找到【Telnet】服务项，该服务项的【启动类型】为已禁用，说明当前主机的 Telnet 服务没有开启，双击【Telnet】服务项，如图 6-2 所示。

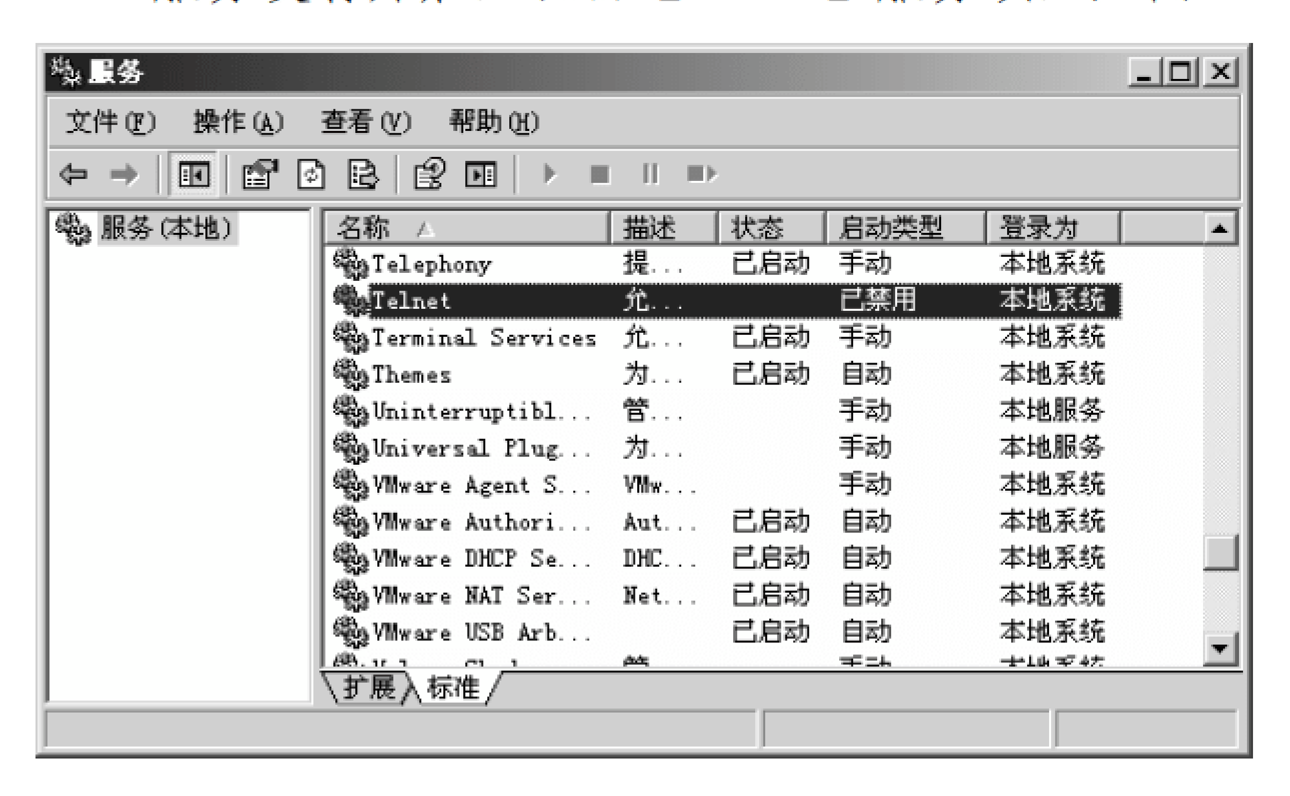


图 6-2

03 弹出【Telnet 的属性】对话框，默认为【已禁用】启动类型，此时的【服务状态】全为灰色。在【启动类型】选项列表中选择【手动】选项，单击【应用】按钮，如图 6-3 所示。



图 6-3

04 【启动类型】变为【手动】，单击【启动】按钮，如图 6-4 所示。

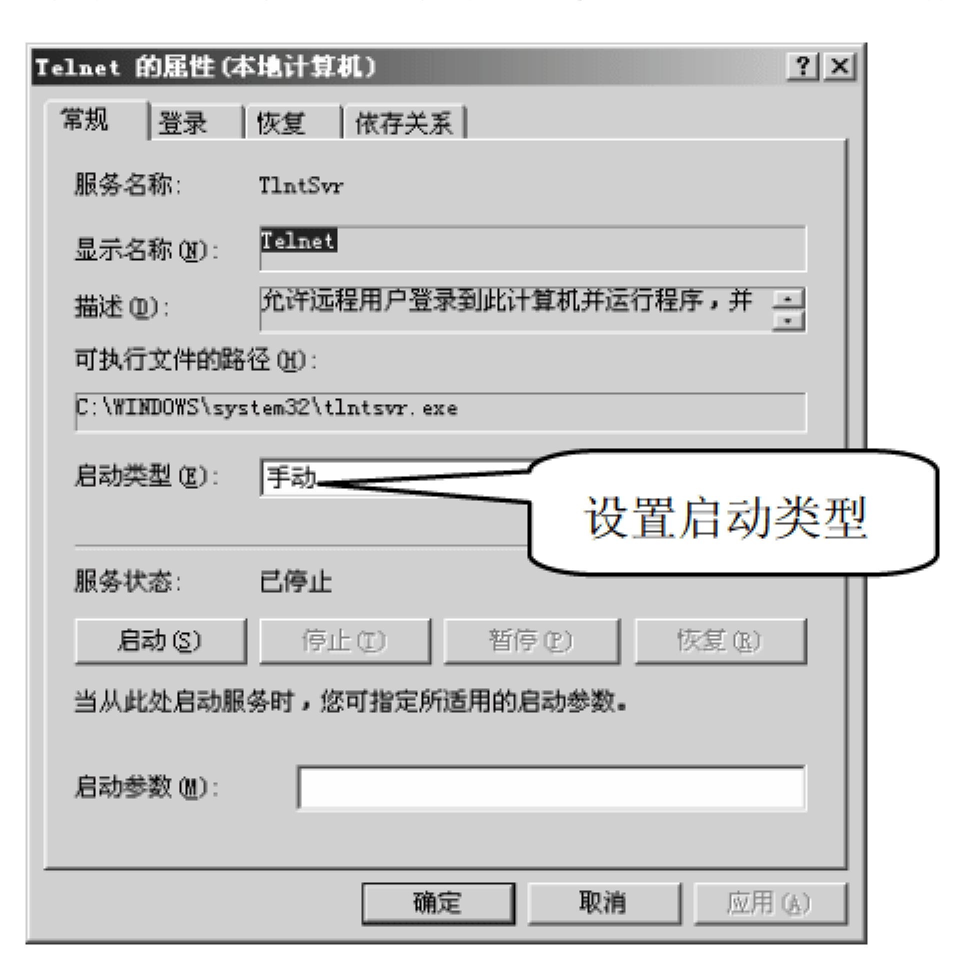


图 6-4

05 【服务状态】为“已启动”，对当前服务状态可以执行【停止】和【暂停】操作，单击【确定】按钮完成 Telnet 服务的开启，如图 6-5 所示。


提 示

控制端和被控制端的 Telnet 服务都开启后，需要在控制端的命令提示符中执行 Telnet 连接命令“telnet ip/hostname”。在连接时必须输入有权限的账户和密码，一般使用管理员账户“administrator”，密码不能为空。



图 6-5

6.3.2　远程桌面

远程桌面功能是 Windows 系统自带的一种远程管理工具。它具有操作方便、直观等特征。当服务器开启了远程桌面连接功能后，就可以在网络中的其它终端客户机上连接控制这台服务器了。通过远程桌面功能可以实时的操作服务器，几乎可以对服务器进行任何操作，就好像是直接在该服务器上操作一样。

但是，Windows 远程桌面使用 IP 地址指向被控端主机进行连接，这在跨网络互联时很不方便，所以很多机构研究出了更安全、易用的远程桌面控制工具，像国内的 51MyPC，国外的 Mikogo 等。

6.3.3　远程控制——RemotelyAnywhere

RemotelyAnywhere 程序是利用浏览器进行远程连接控制服务器的小程序。使用时只需要在服务器端安装该软件即可，只要知道连接地址及端口，其他任何主机都可以通过浏览器访问，不过该软件的部分功能需要支持 JAVA 的浏览器才能实现。

通过该软件可以轻松直观的获取任何管理、性能信息，可以对服务器进行完全的控制。由于只需要在服务器上安装程序，所以管理员即使在互联网也可以访问内网的管理服务器，前提是该服务的地址端口能通过出口设备的 NAT 转换功能被外网访问。

6.3.4　远程控制——pcAnywhere

和 RemotelyAnywhere 比起来，PcAnywhere 的操作就有些复杂了。该软件在使用时需要在管理端和被管服务器端都安装 PcAnywhere 程序。实现服务管理后，也可以实现服务器的完全控制。虽然麻烦些，但是相对 RemotelyAnywhere 却显得更安全。

6.4 项目实施 1：使用 51MyPC 轻松管理办公室中的电脑

51MyPC 软件主要是为商务精英及 SOHO 一族设计的，使用户轻松享受远程办公生活，由于它的方便、快捷、安全，完全可以应用于远程服务器管理，特别是网络管理员在出差时。使用这个软件还有一个好处，就是不需要记忆被管设备的地址，只要通过其官网输入为被管设备设定的设备名、密码即可。下面详细介绍 51MyPC 的使用方法。

1. 在被控制的计算机上安装 51MyPC

首先需要在被控制服务器上安装 51MyPC 软件，具体的操作步骤如下。

01 运行 51MyPC 安装程序，弹出【欢迎使用 51MyPC 安装程序】对话框，单击【下一步】按钮，如图 6-6 所示。

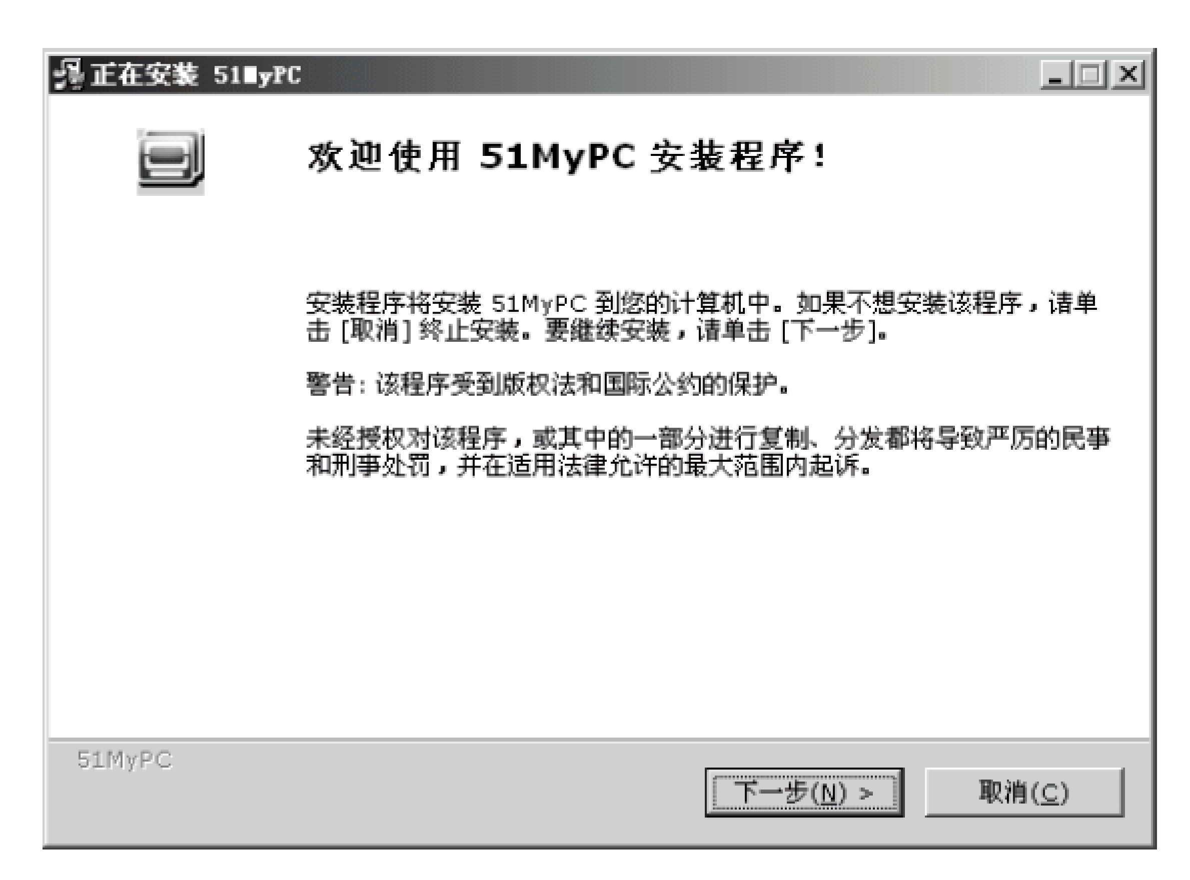


图 6-6

02 弹出【目标文件夹】对话框，在其中可以设置安装目录，单击【浏览】按钮更改目录位置，本实例采用默认配置，单击【下一步】按钮，如图 6-7 所示。

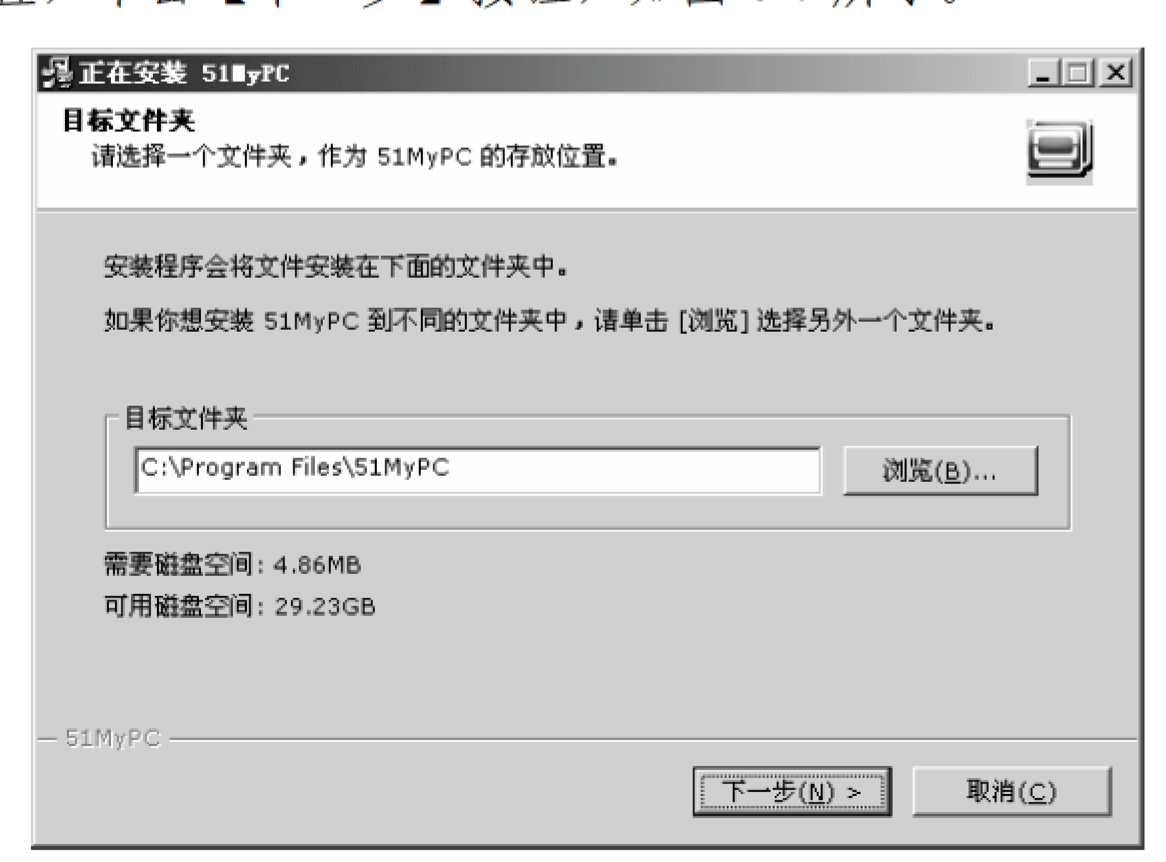


图 6-7

03 弹出【账户信息】对话框，在其中配置连接账户，客户端通过该账户即可远程连接服务

器，对应内容输入完成后单击【下一步】按钮，如图 6-8 所示。

图 6-8

04 弹出【电脑信息】对话框，在【计算机昵称】文本框中输入远程连接时显示的计算机名，本实例使用“server1”，单击【网络配置】按钮，如图 6-9 所示。



图 6-9

05 弹出【网络配置】对话框，在其中可以设置本服务器联网的代理服务器配置，本实例采用默认配置，单击【登陆】按钮，如图 6-10 所示。



图 6-10

06 程序安装成功，弹出客户端连接教程页面，如图 6-11 所示。



图 6-11

2．在控制端连接被控服务器

当客户机想连接远程已安装 51MyPC 程序的服务器时，需要登陆该程序的官网进行连接，客户端远程桌面连接服务器的具体操作步骤如下。

01 进入 51MyPC 官方网站，单击首页的【登录】超级链接，如图 6-12 所示。



图 6-12

02 进入客户端登录界面，在【Email】和【密码】对话框中分别输入服务器端安装程序使用的邮箱及密码，单击【登录】按钮，如图 6-13 所示。



图 6-13

03 进入【计算机管理中心】页面，通过该页面可以设置远程桌面的色彩、分辨率、声音、3D 效果等内容，本实例采用默认配置，单击【远程控制】按钮，如图 6-14 所示。

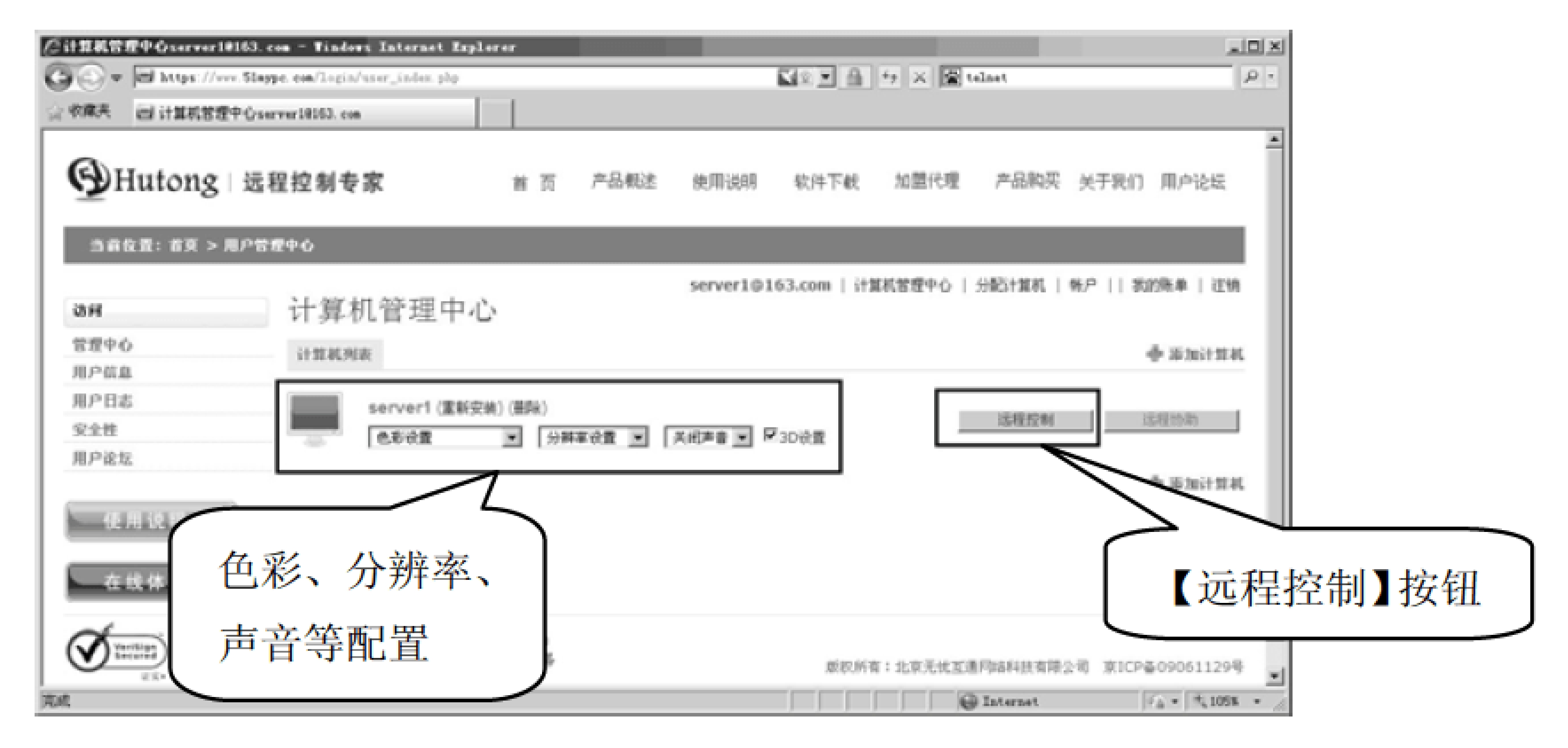


图 6-14

04 进行远程控制，需要有控件支持，根据提示页面的操作方法，为此计算机安装控件，如图 6-15 所示。

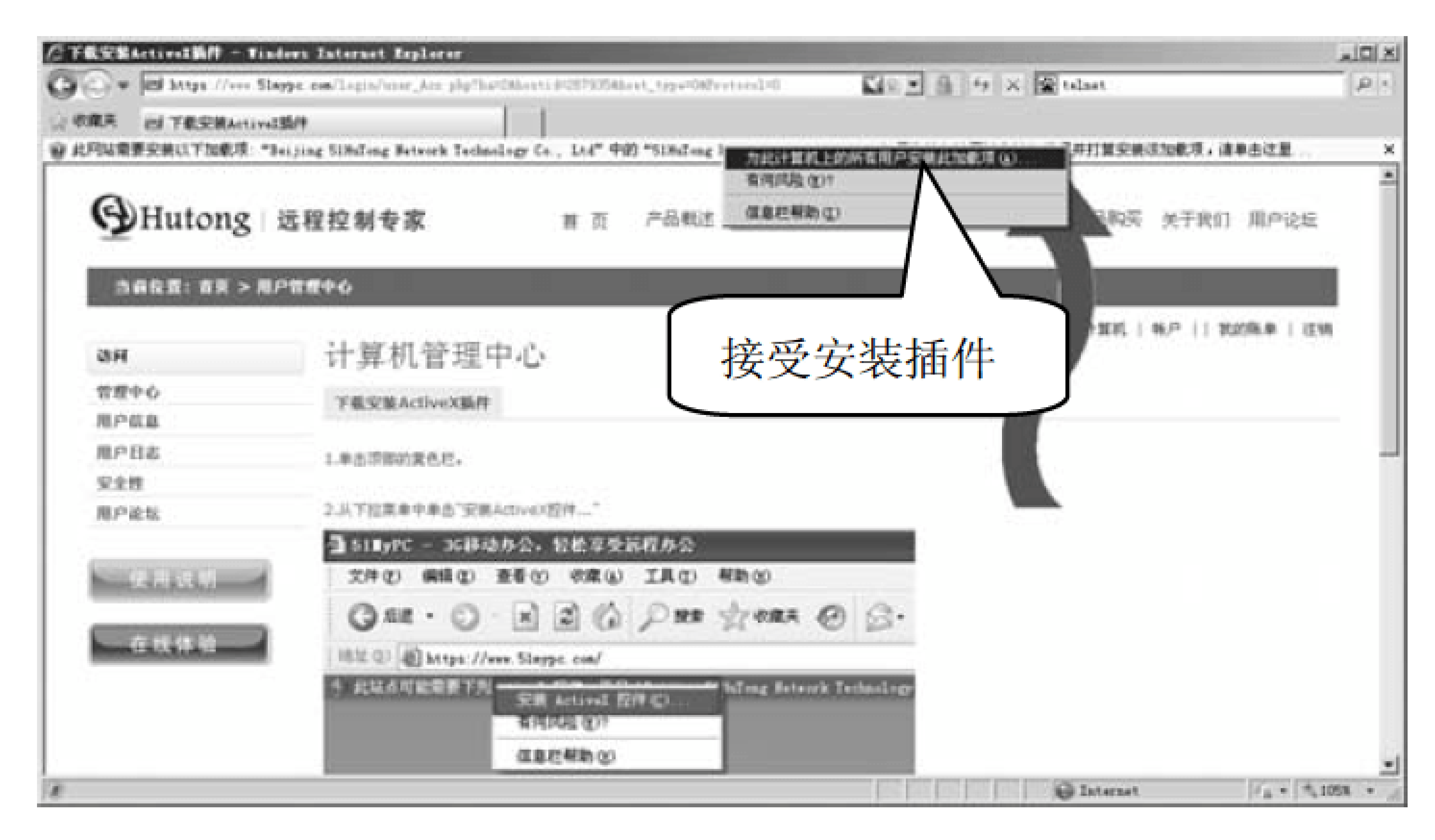


图 6-15

05 弹出控件安装对话框，单击【安装】按钮，如图 6-16 所示。



图 6-16

06 弹出远程桌面连接程序，系统自动验证，并建立连接，如图 6-17 所示。



图 6-17

07 验证连接成功，弹出远程主机系统登录界面，输入有效账户及密码，单击【确定】按钮，如图 6-18 所示。

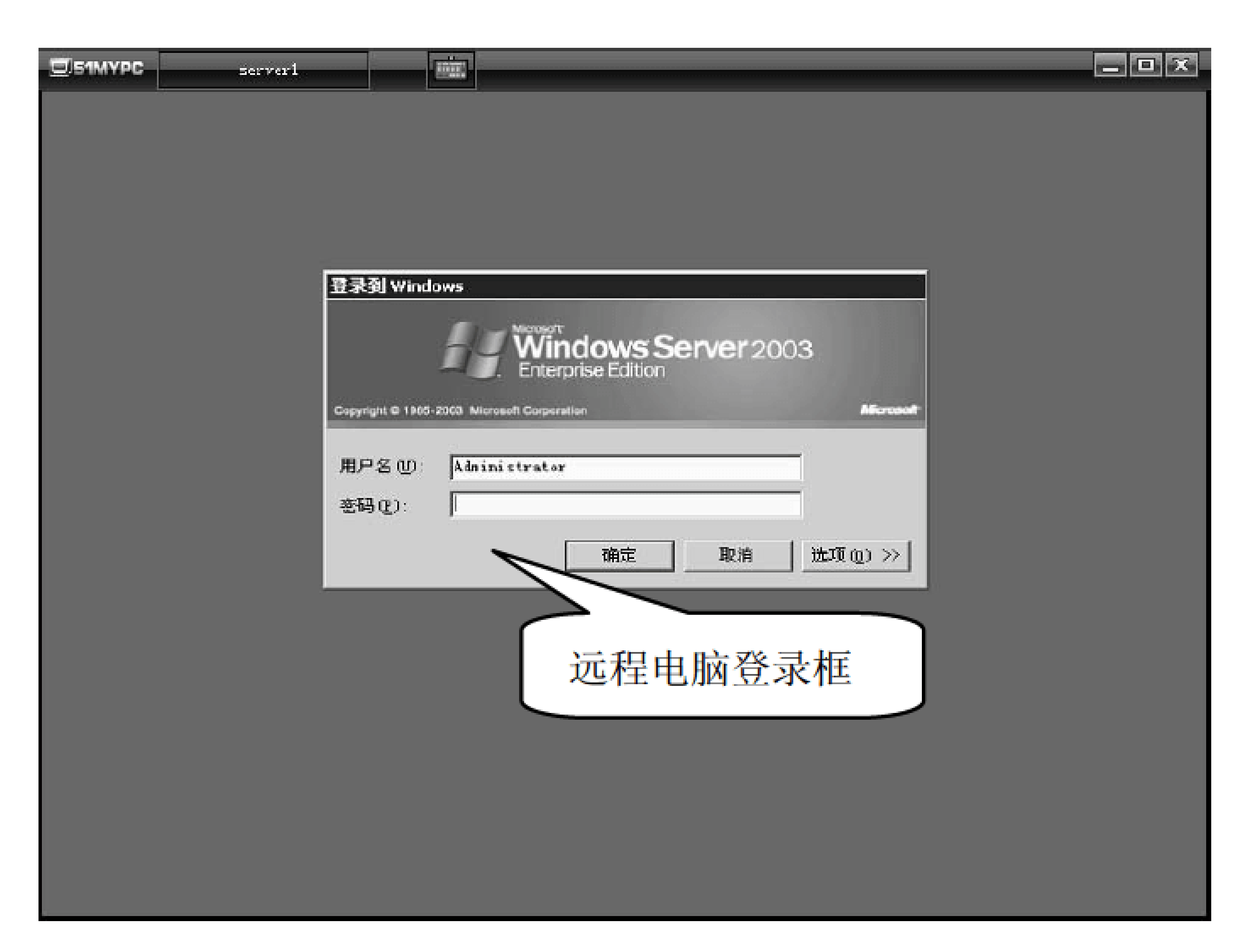


图 6-18

08 登录成功，进入远程主机桌面，下面可对远程主机实施管理操作，如图 6-19 所示。



图 6-19

6.5 项目实施 2：使用 RemotelyAnywhere 远程管理服务器

使用 RemotelyAnywhere 工具实现服务器远程管理时，需要考虑管理员是否需要在外网访问。如果需要，必须要从网络出口设备上得到此设备的访问地址做 NAT 地址转换。

下面详细介绍 RemotelyAnywhere 工具的安装及应用方法。

6.5.1 安装 RemotelyAnywhere

通过官方网站，可以获得 RemotelyAnywhere 最新版本的安装程序。其具体的安装操作步骤如下。

01 运行 RemotelyAnywhere 安装程序，在弹出的对话框中单击【Next】（下一步）按钮，如图 6-20 所示。



图 6-20

02 弹出【Terms and Conditions of Use】（使用的条款和条件）对话框，单击【I Agree】（我同意）按钮，如图 6-21 所示。

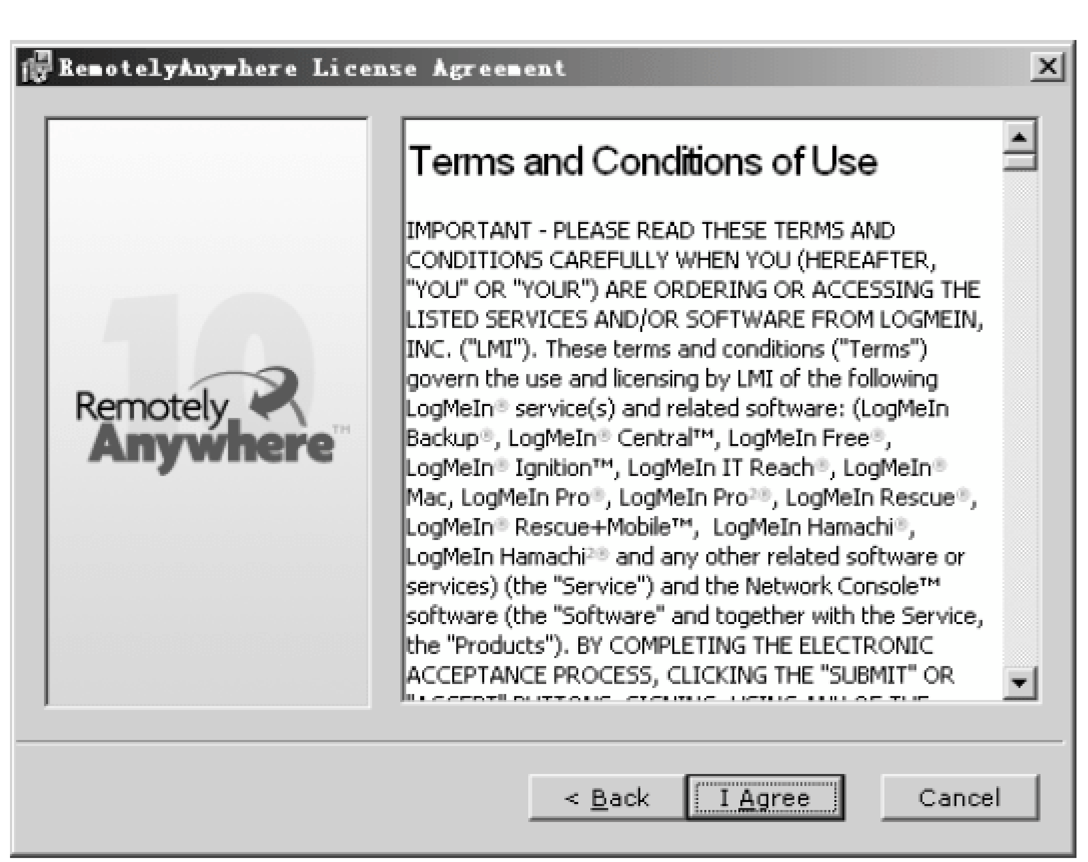


图 6-21

03 弹出【Software options】（软件配置）对话框，如果选择【Custom】（自定义）单选按钮，可以手工指定软件安装配置项，本实例选择【Typical】（典型）单选按钮，使用默认配置，单击【Next】（下一步）按钮，如图 6-22 所示。



图 6-22

04 弹出【Choose Destination Location】（改变目录位置）对话框，单击【Browse】（浏览）按钮可以改变安装目录，本实例采用默认配置，单击【Next】（下一步）按钮，如图 6-23 所示。

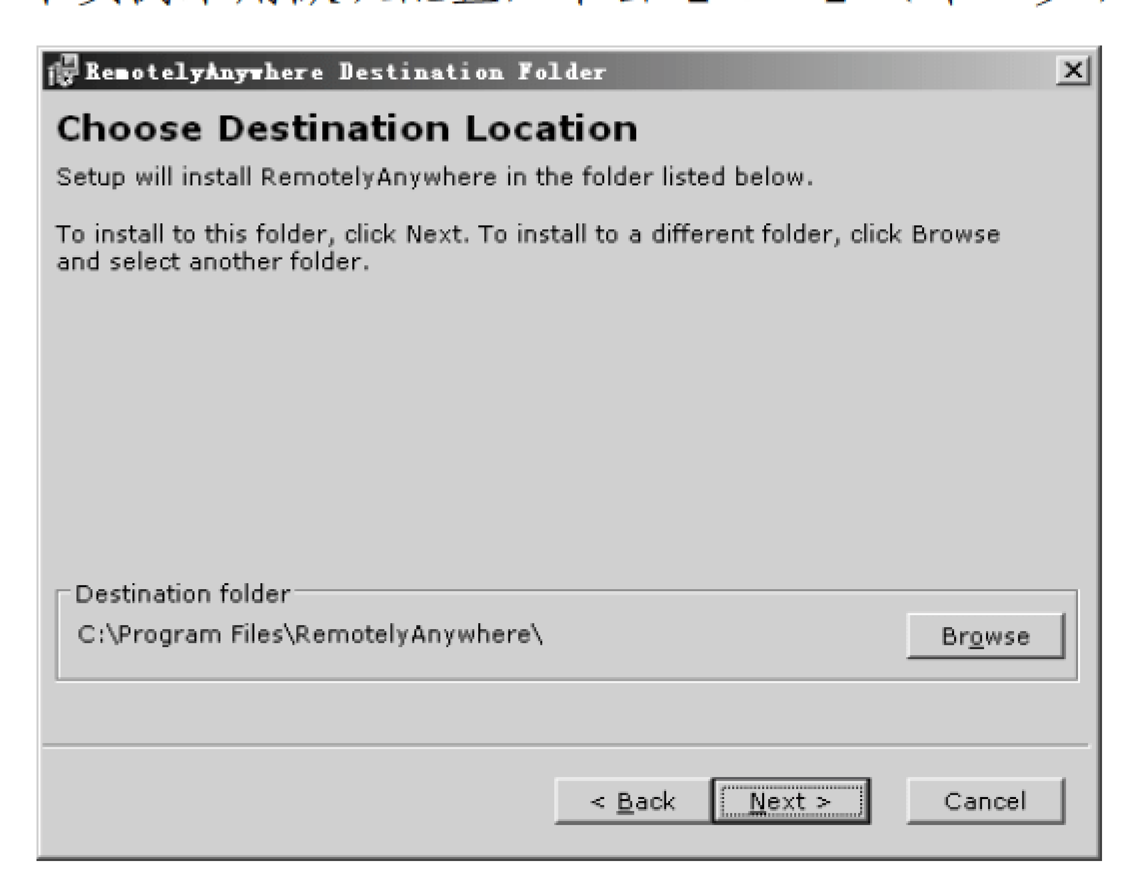


图 6-23

05 弹出【Start copying files】（开始复制文件）对话框，显示已配置信息，信息中说明连接服务器的端口为“2000”，单击【Next】（下一步）按钮，如图 6-24 所示。



图 6-24

06 弹出【Install status】（安装状态）对话框，系统自动安装 RemotelyAnywhere 程序，如图 6-25 所示。



图 6-25

07 安装完成后，弹出【Setup Completed】（安装完成）对话框，对话框中标明可以使用地址“http://20110211-1604:2000”和“http://ipaddress:2000”连接服务器，单击【Finish】（完成）按钮，如图 6-26 所示。



图 6-26

08 RemotelyAnywhere 安装完成之后需要激活，打开 RemotelyAnywhere 运行程序，在弹出的对话框中单击【请单击此处以激活 RemotelyAnywhere】超级链接，如图 6-27 所示。

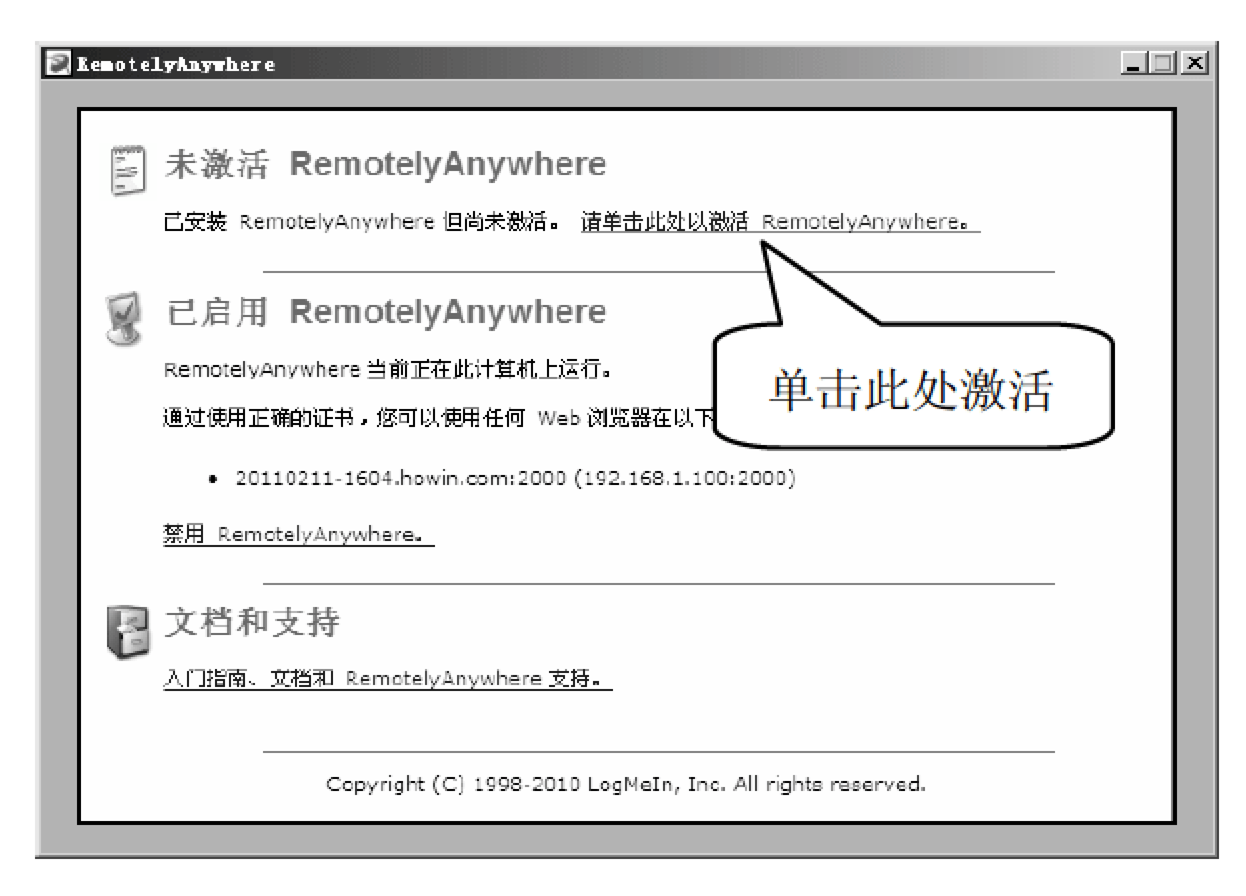


图 6-27

09 弹出 RemotelyAnywhere 激活方式选择页面，可以选择【我已是 RemotelyAnywhere 用户或已具有 RemotelyAnywhere 许可证】单选按钮进行激活，也可以选择【我希望现在购买 RemotelyAnywhere】在线激活，本实例选择【我想免费试用】单选按钮激活试用，单击【下一步】按钮，如图 6-28 所示。



图 6-28

10 在弹出的页面的【电子邮件地址】文本框中输入激活使用的邮箱地址，并在【产品类型】列表选项中选择试用产品类型，本实例采用“服务器版”，单击【下一步】按钮，如图 6-29 所示。



图 6-29

11 在弹出的页面中依次输入指定内容，单击【下一步】按钮，如图 6-30 所示。

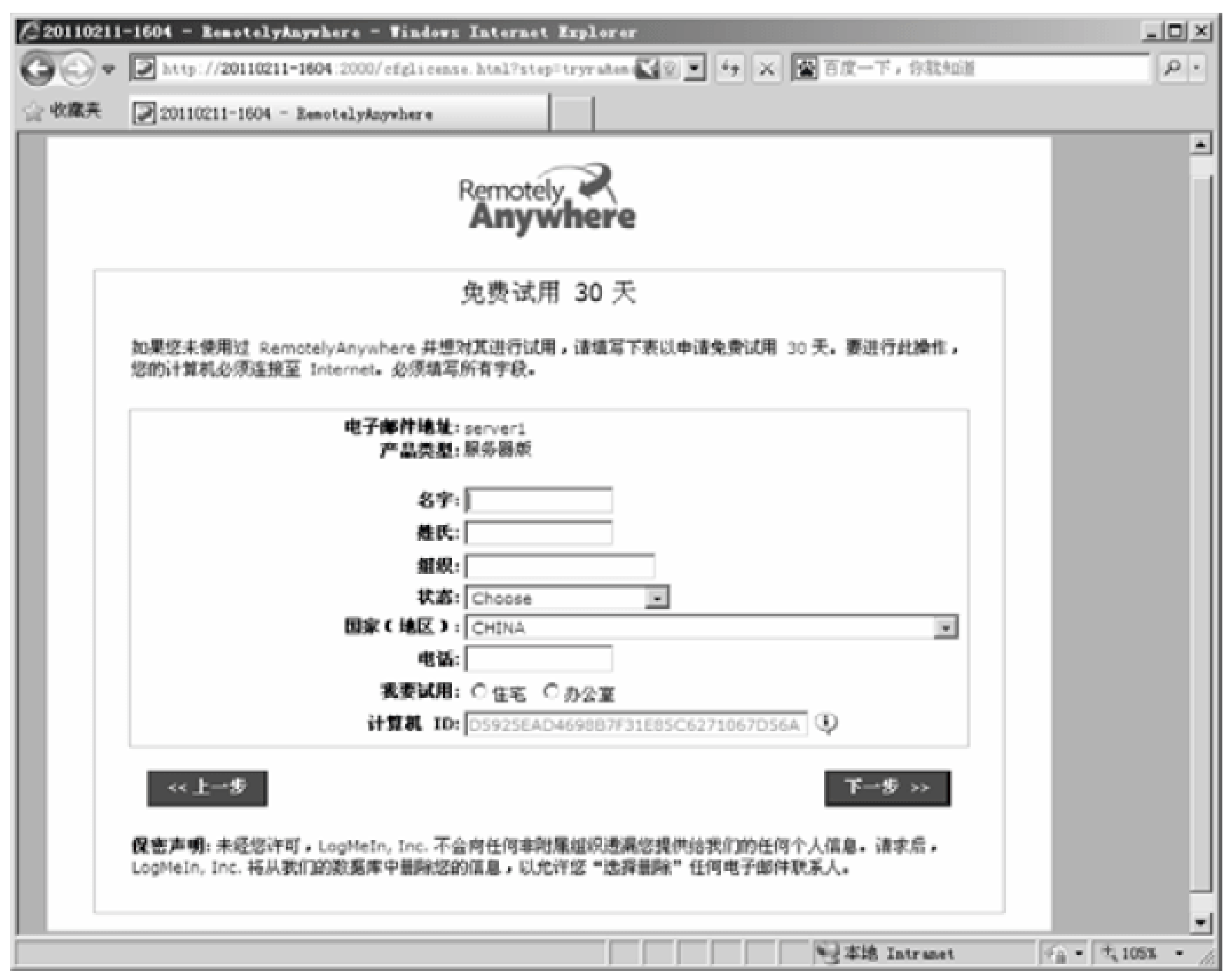


图 6-30

12 RemotelyAnywhere 激活成功，需要重新启动 RemotelyAnywhere 程序，单击【重新启动 REMOTELYANYWHERE】按钮，如图 6-31 所示。



图 6-31

6.5.2 实时监控服务器性能

可以在任何远程主机中使用浏览器监控安装了 RemotelyAnywhere 的服务器，下面详细介绍如何利用该工具监控远程服务器。

首先用户需要登录 RemotelyAnywhere 管理页面，具体操作步骤如下。

01 在客户端主机打开 IE 浏览器，在地址栏中输入 RemotelyAnywhere 安装过程中提示的地址，通用格式为“http://{目标服务器 ip|主机名|域名}:2000”，本实例使用“http://192.168.1.100:2000”进行讲解。在弹出的页面中选择【Show advanced options >>】（查看高级选项）按钮，如图 6-32

所示。

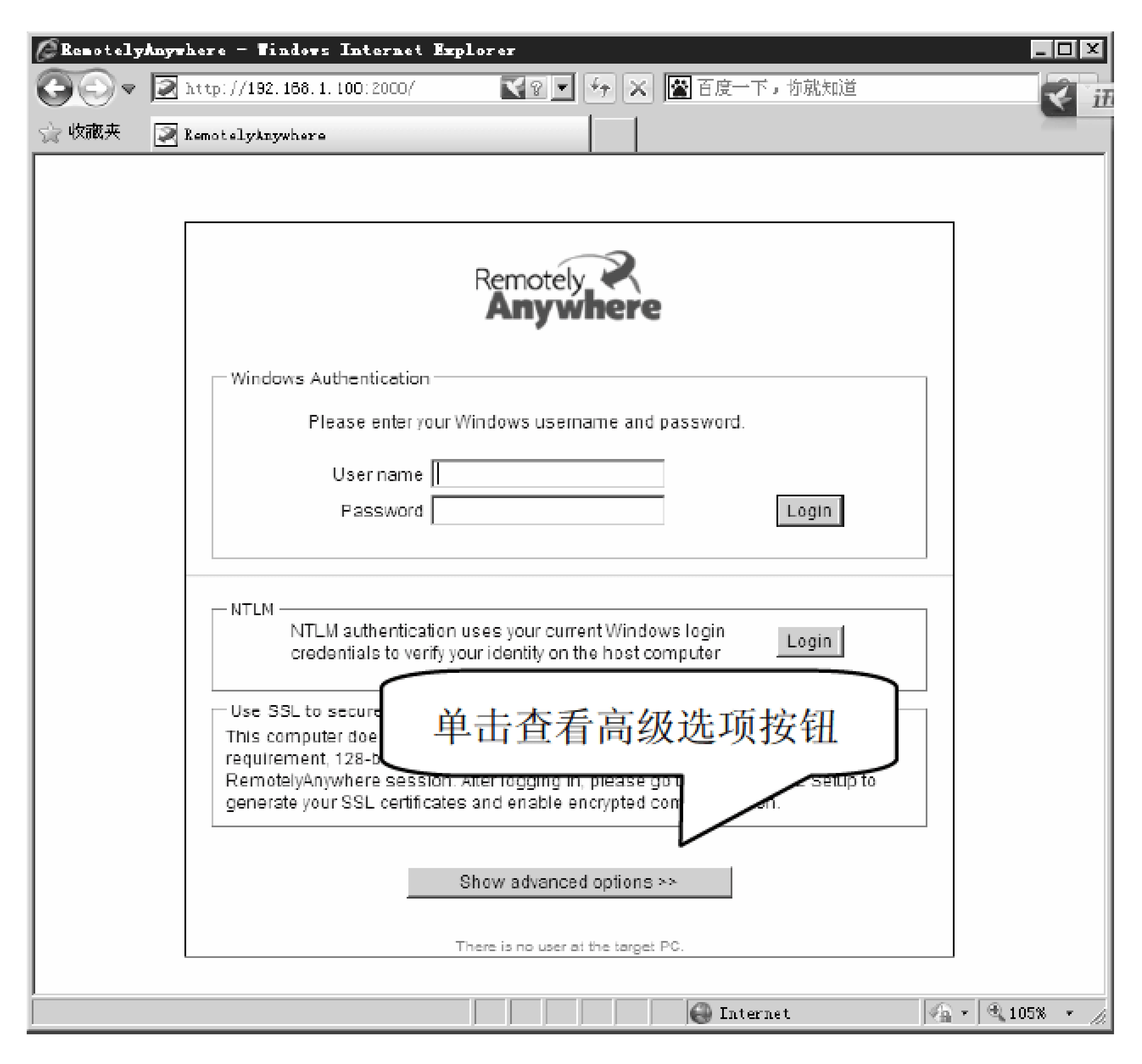


图 6-32

02 页面下方显示出高级选项内容，在【Select language】（设置语言）列表选项中选择【中文（简体）】选项，如图 6-33 所示。

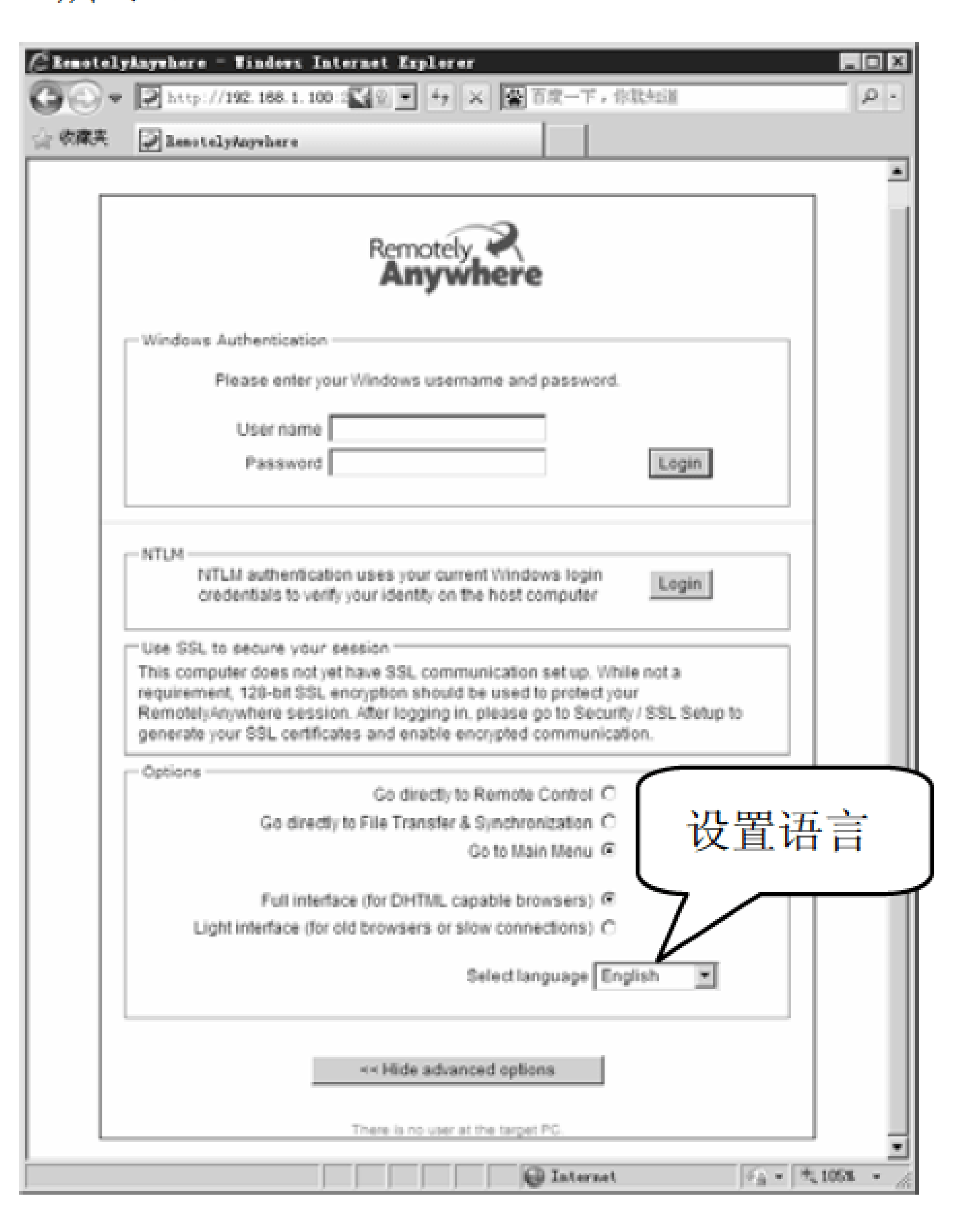


图 6-33

03 页面变成中文显示，在【用户名】和【密码】文本框中输入有效远程管理账户的信息，默认使用 administrator 账户登录，单击【登录】按钮，如图 6-34 所示。

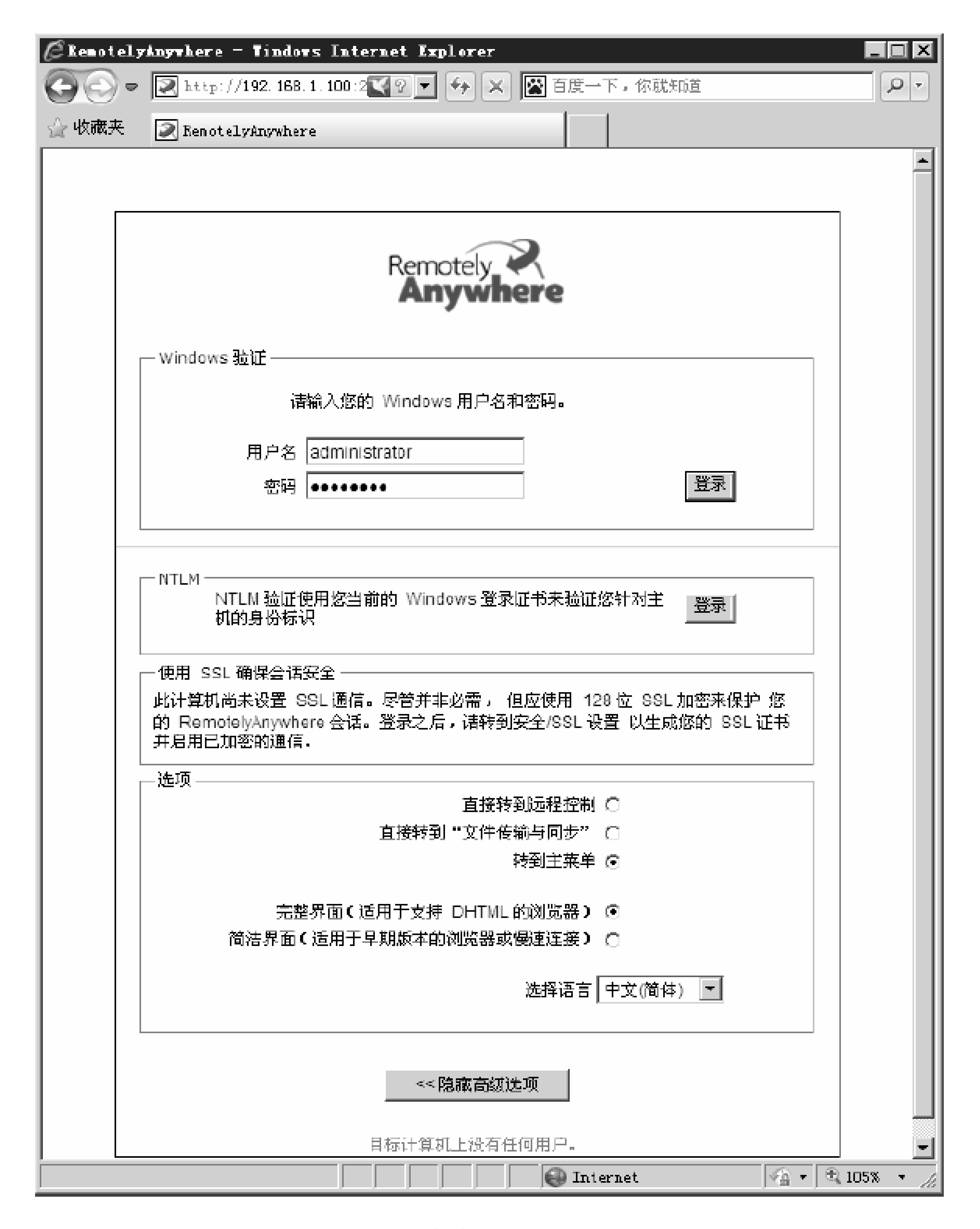


图 6-34

04 进入 RemotelyAnywhere 远程管理界面，单击【继续】按钮进行远程服务器信息查看与管理，如图 6-35 所示。



图 6-35

进入 RemotelyAnywhere 管理界面后，左侧出现管理功能列表，管理员可以使用不同的管理功能对远程服务器进行多功能全方位的管理操作。

1. 通过控制面板快速了解系统信息

进入 RemotelyAnywhere 后，默认显示【控制面板】管理功能页面，如图 6-36 所示。通过该页面可以快速的了解远程服务器的多种状态、信息，具体内容如下。

- 系统信息：显示系统版本、CPU 型号、物理内存使用情况、总内存（包括虚拟内存）使用情况、系统已启动时间、登录系统账户。
- 事件：显示最近发生的系统事件，默认显示五个事件。
- 进程：显示进程的系统资源占用情况，默认以 CPU 占用比例为序，显示 CPU 占用最多的五个进程。
- 已安装的修补程序：最近安装的系统补丁，默认显示五个补丁信息。
- 网络流量：动态显示网络流量信息。
- 磁盘驱动器：所有分区的空间使用情况。
- 计划的任务：显示最后执行的任务计划，默认为五个。
- 最近的访问：系统最近访问记录。
- 日记：管理员可在此区域编辑管理日记。

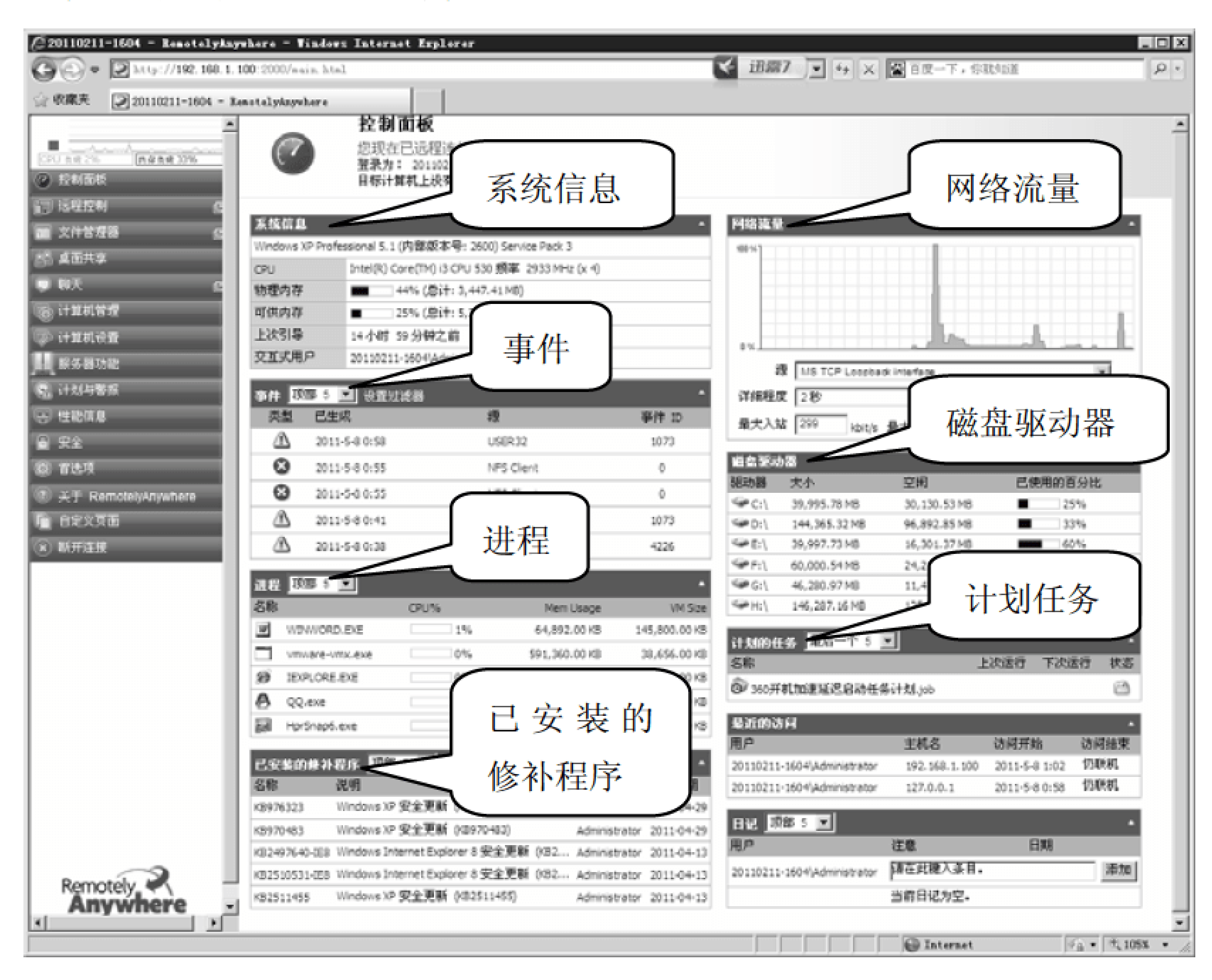


图 6-36

2. 远程操控服务器

选择左侧列表中的【远程控制】选项，在右侧窗格中显示了远程服务器的界面，通过该窗格可以利用本地的鼠标、键盘、显示器直接控制远程主机。在窗格上侧有部分工具可以使用，包括颜色调整、远程桌面大小调整等，如图 6-37 所示。



图 6-37

3. 文件管理器

选择左侧列表中的【文件管理器】选项，在右侧窗格中显示了本地和远程主机的资源管理器，在两个资源管理器中可以随意的拖曳文件，以实现资料互传，如图 6-38 所示。

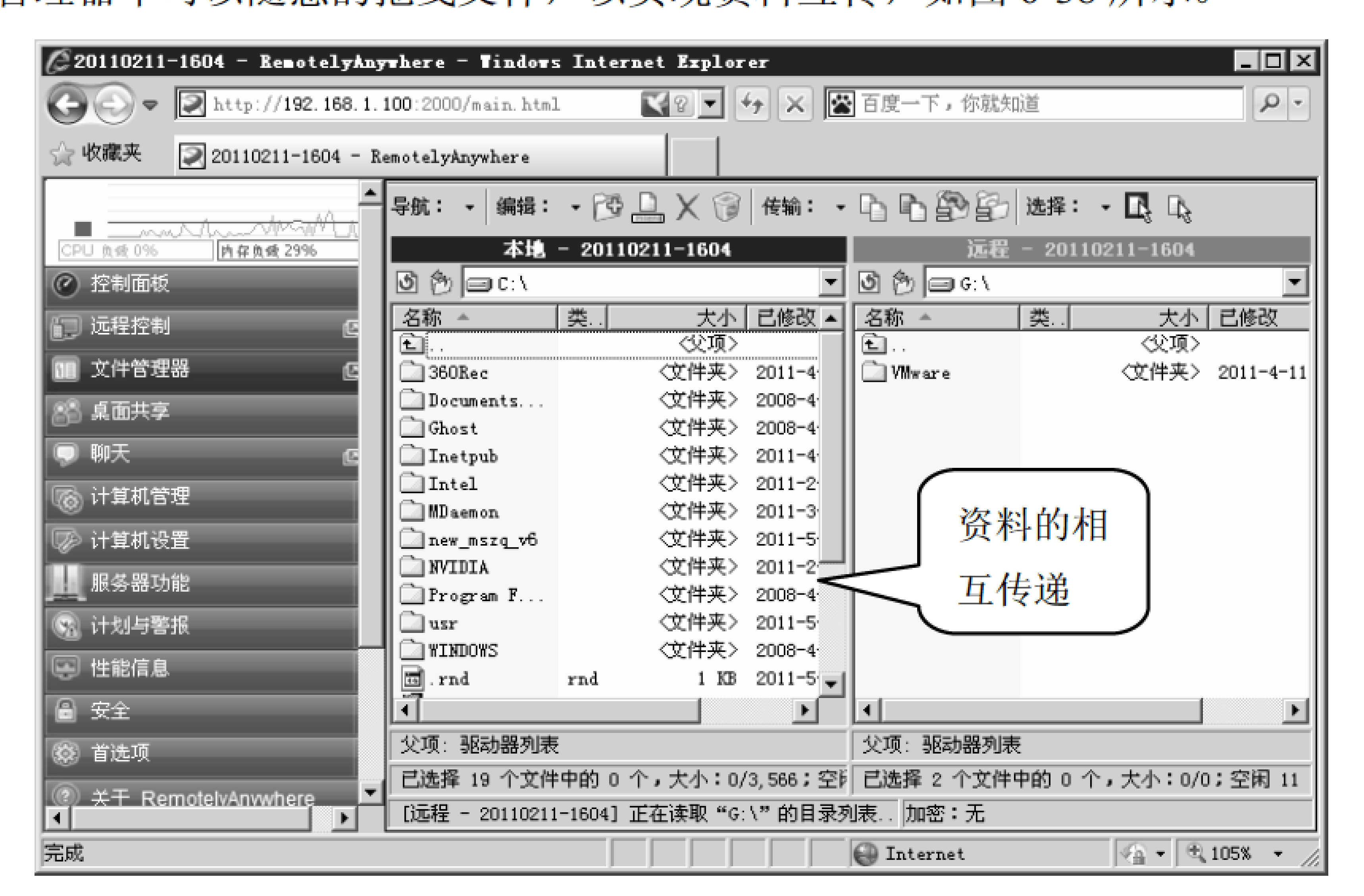


图 6-38

4. 桌面共享

通过该功能可以邀请其他主机对远程服务器进行监控。一般当管理员无法完成一些操作时，可以通过该功能邀请其他技术人员帮忙解决。

具体的操作步骤如下。

01 选择左侧列表中的【桌面共享】选项，在右侧窗格中显示了实现桌面共享的操作方法。按照提示方法右击桌面状态栏的程序图标，在弹出的快捷菜单中选择【Share my Desktop...】（共享我的桌面）菜单命令，如图 6-39 所示。



图 6-39

02 弹出【桌面共享】对话框，选择【邀请来宾与您一起工作】单选按钮，单击【下一步】按钮，如图 6-40 所示。

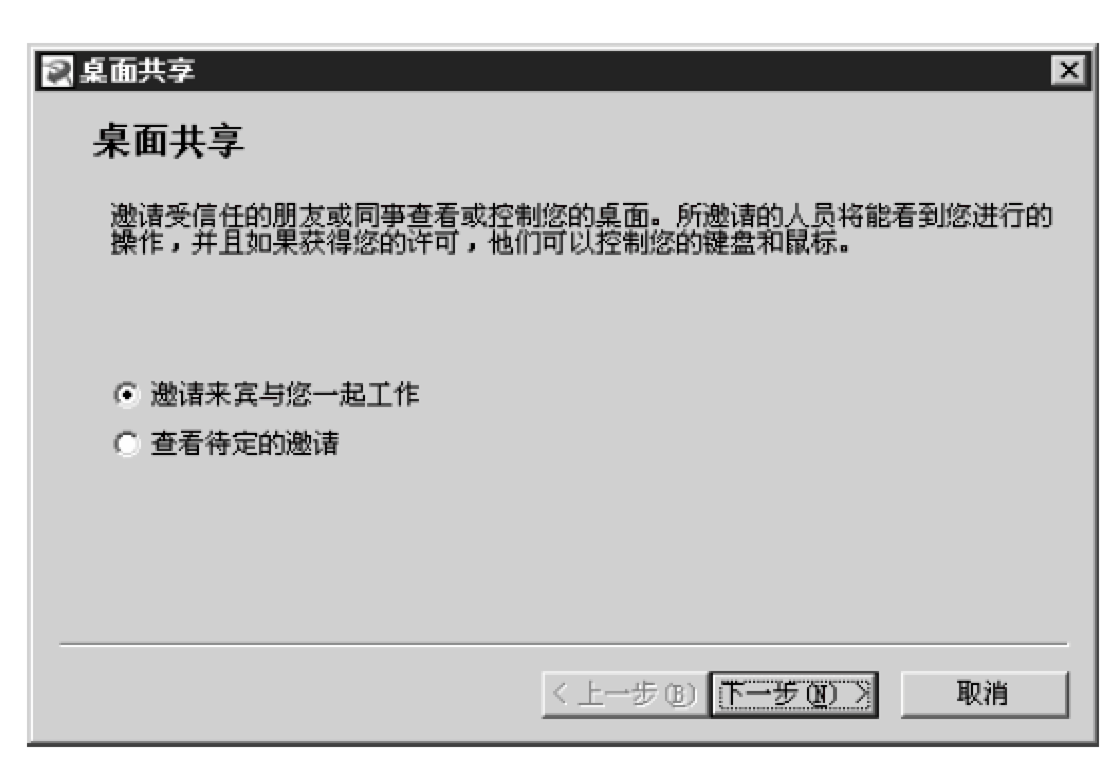


图 6-40

03 弹出【邀请详情】对话框，可以在本对话框中配置邀请名，默认按时间显示，方便以后查看，还可以设置本次邀请的有效访问时限，在最后一个文本框中输入被邀请人连接服务器使用的地址，全部选择默认配置，单击【下一步】按钮，如图 6-41 所示。

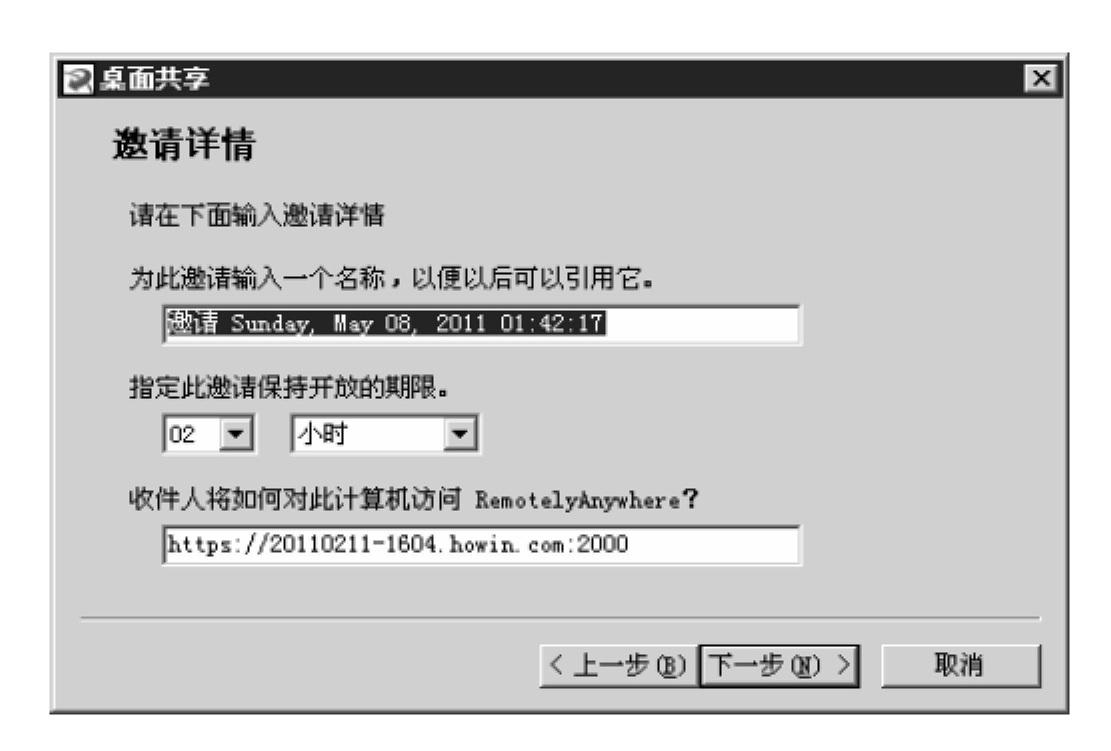


图 6-41

04 弹出【已创建邀请】对话框，在文本框中显示了被邀请人获得的地址，可以通过单击【复制】和【电子邮件】两个按钮，让被邀请人获得邀请地址，单击【完成】按钮，完成本次邀请，如图 6-42 所示。

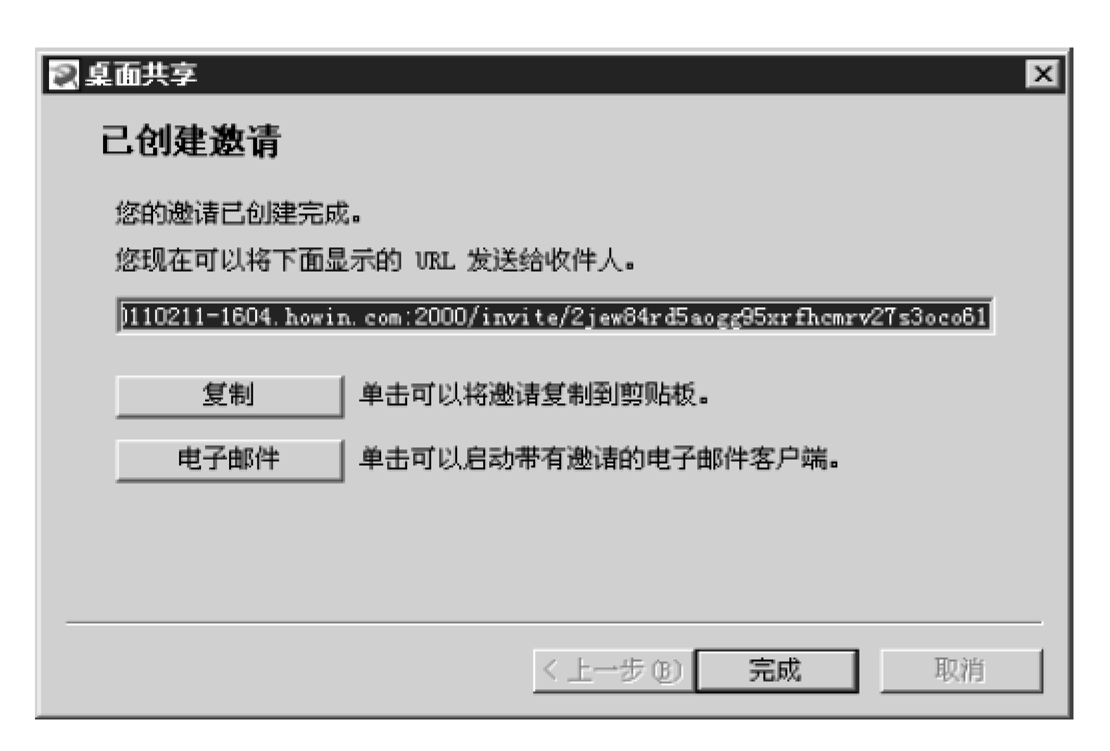


图 6-42

5. 聊天功能

在左侧选项列表中选择【聊天】选项，通过右侧窗格可以和被管设备聊天，一般被管设备很少有人在，所以该功能用的比较少，如图 6-43 所示。

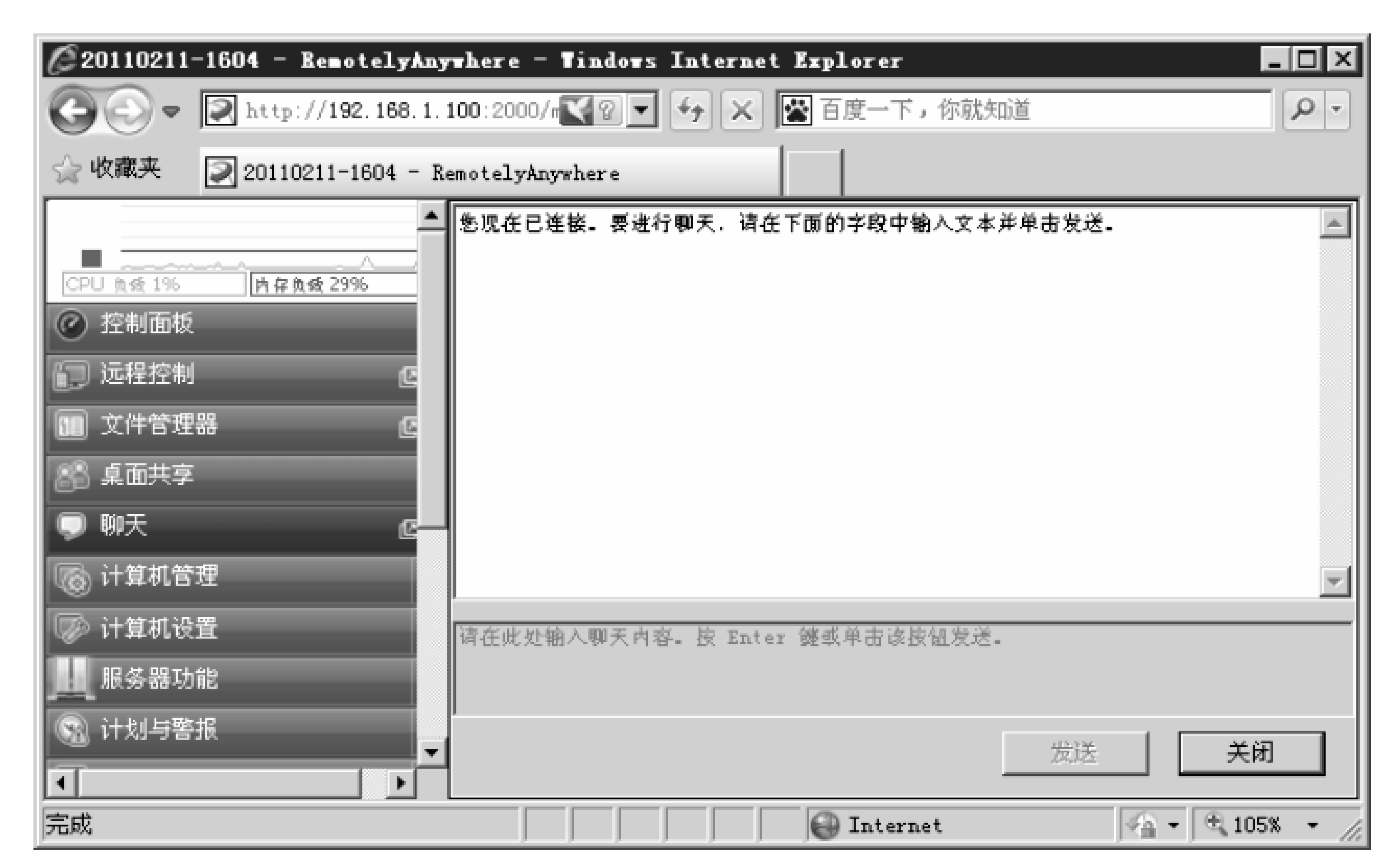


图 6-43

6. 计算机管理

可以对远程服务器实现用户管理、事件查看器、服务、进程、驱动程序、注册表编辑器等多种计算机管理功能。下面分别做介绍。

（1）用户管理

选择左侧列表中的【计算机管理】➢【用户管理器】选项，在右侧【用户管理器】窗格中显示了远程服务器的用户和组信息，单击【添加用户】按钮可以为远程服务器增加用户。同时可以单击用户名对其进行编辑，如图 6-44 所示。



图 6-44

（2）事件查看器

选择左侧列表中的【计算机管理】➢【事件查看器】选项，在右侧窗格中显示了【事件查看器】窗格，通过该窗格可以查看远程服务器的事件信息，如图 6-45 所示。

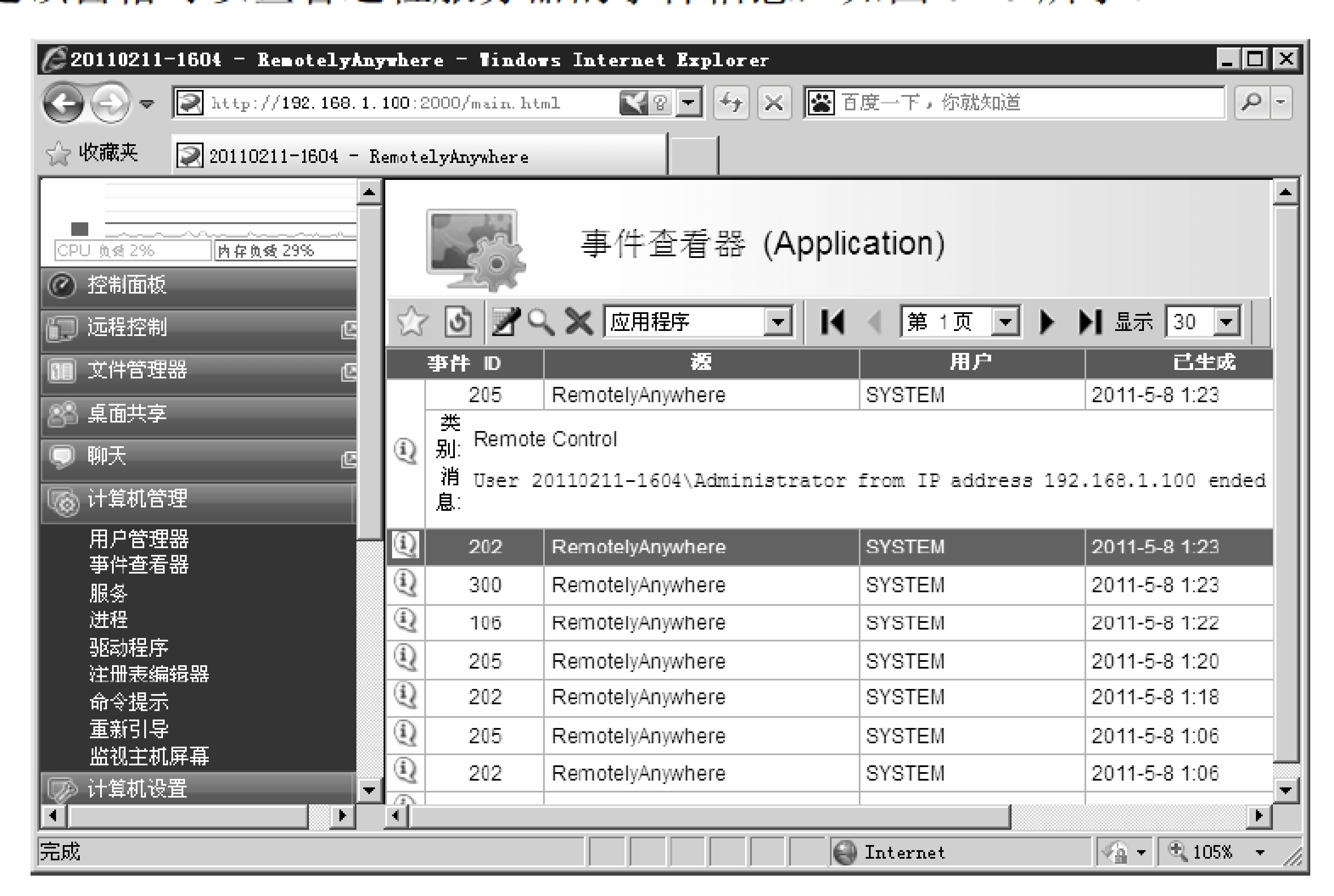


图 6-45

（3）服务

选择左侧列表中的【计算机管理】➢【服务】选项，在右侧窗格中显示了【服务】窗格，通过该窗格可以查看远程服务器所有的服务项，也可以单击这些服务项进行启动、禁用或删除操作，如图 6-46 所示。

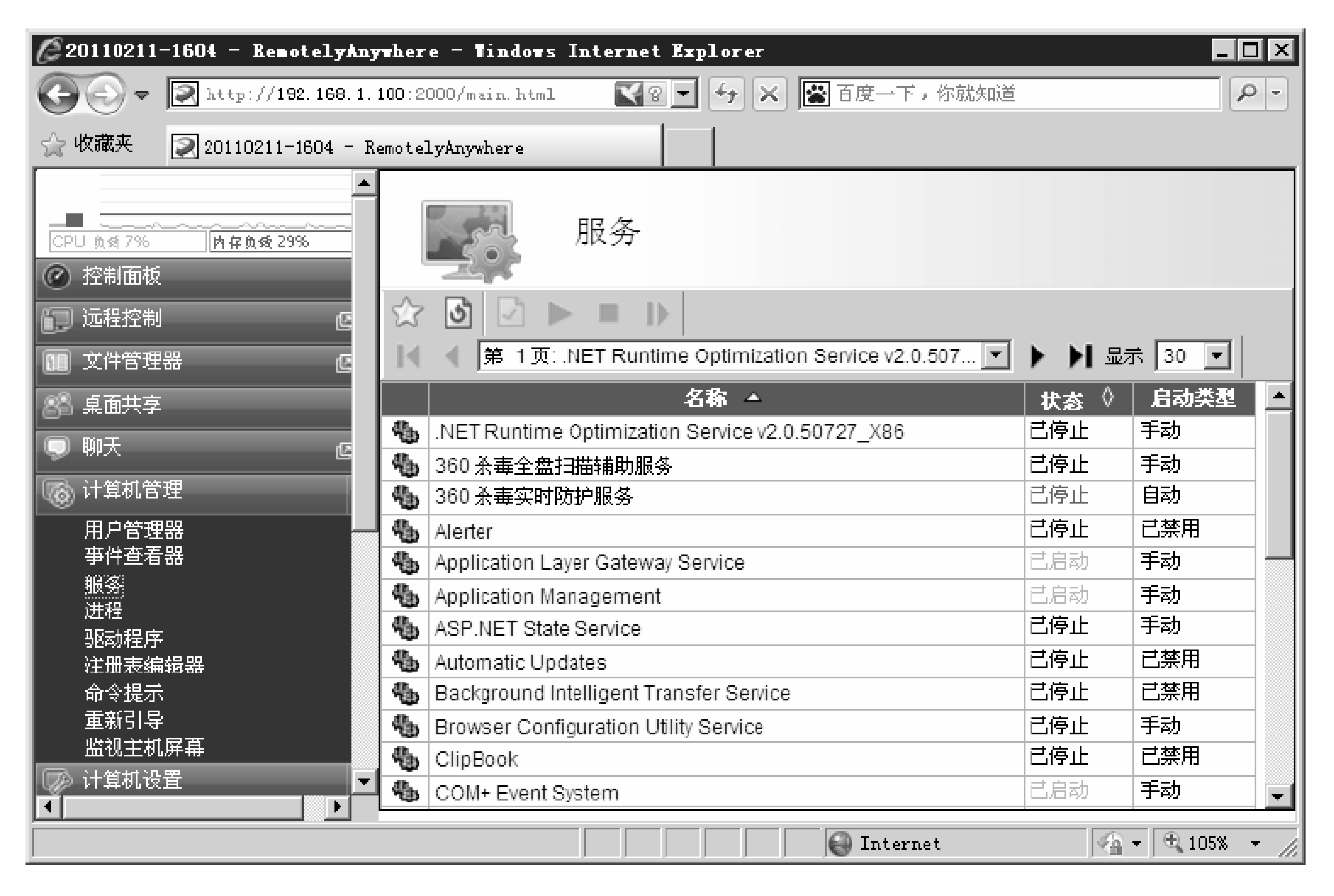


图 6-46

（4）进程

查看进程的具体操作步骤如下。

01 选择左侧列表中的【计算机管理】➢【进程】选项，在右侧窗格中显示了【进程】窗格，通过该窗格可以查看远程服务器所有的进程项，单击进程 PID 号为“1624”的进程，如图 6-47 所示。

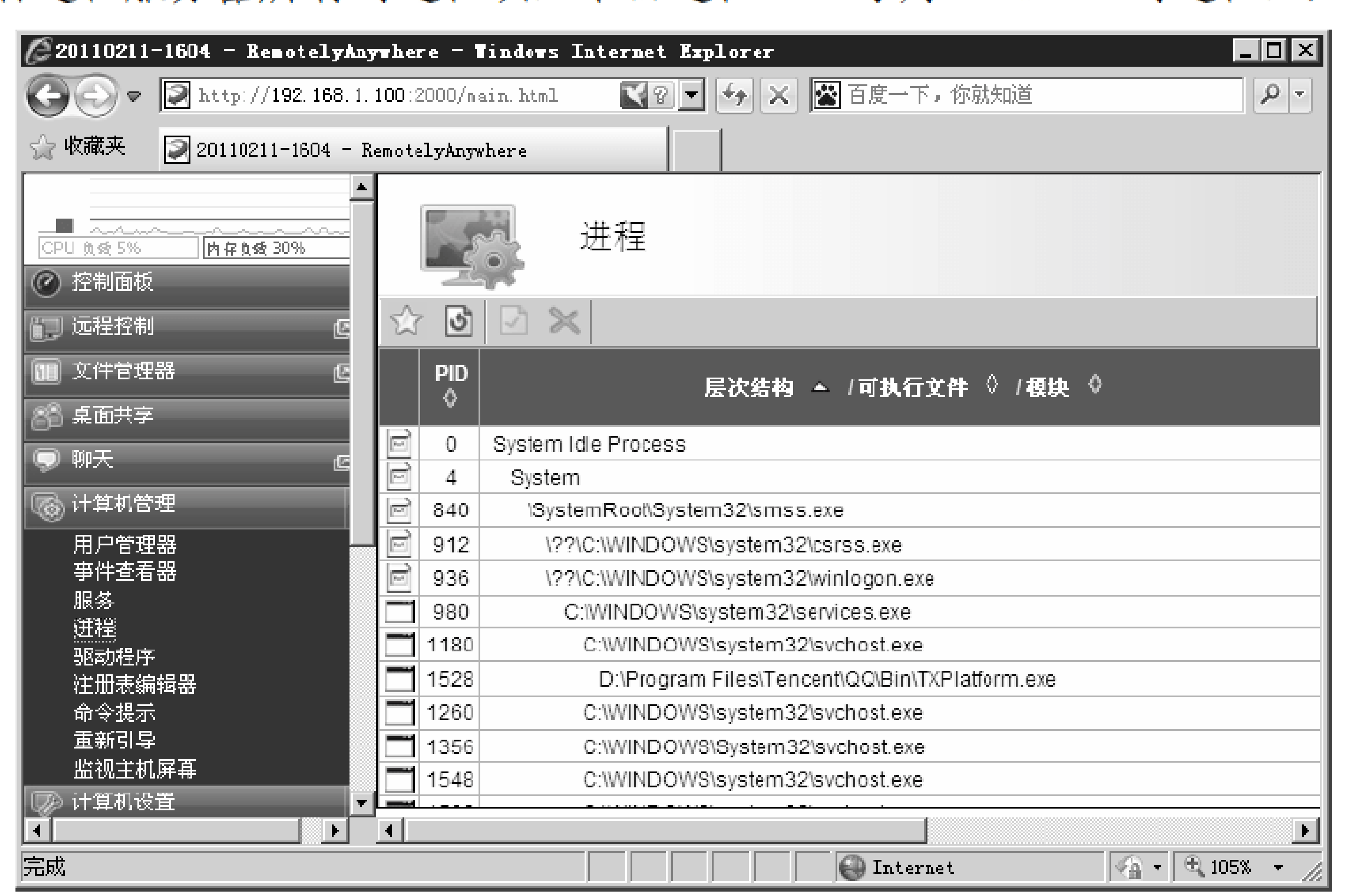


图 6-47

02 弹出新页面，显示出进程 1624 的进程名为 zhudongfangyu.exe，同时还显示了该进程的其他信息，通过【优先级类】下拉菜单选项可以调整该进程的优先级别，为需要优先执行的进程做调整，如图 6-48 所示。



图 6-48

（5）注册表编辑器

选择左侧列表中的【计算机管理】➢【注册表编辑器】选项，在右侧窗格中显示了【注册表编辑器】窗格，通过该窗格可以查看远程服务器的注册表信息，但是默认被隐藏的注册表信息无法看到，如【HKEY_LOCAL_MACHINE】➢【SAM】➢【SAM】下的系统账户注册表信息，如图 6-49 所示。

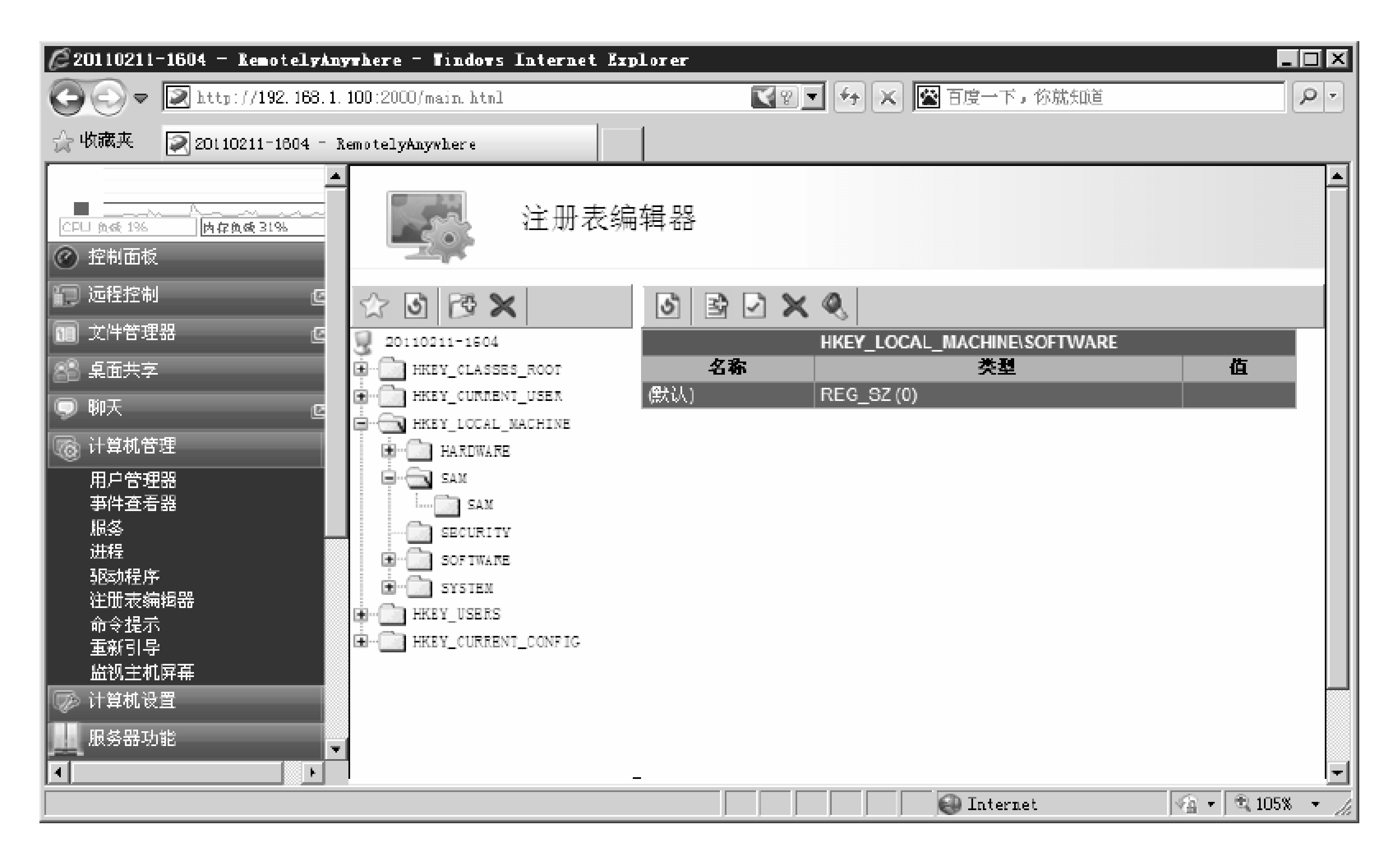


图 6-49

（6）命令提示

选择左侧列表中的【计算机管理】➢【命令提示】选项，在右侧窗格中显示了【命令提示】窗格，通过该窗格可以使用命令对远程服务器进行操作，这对喜欢使用命令管理的管理员来说很有

用，如图 6-50 所示。

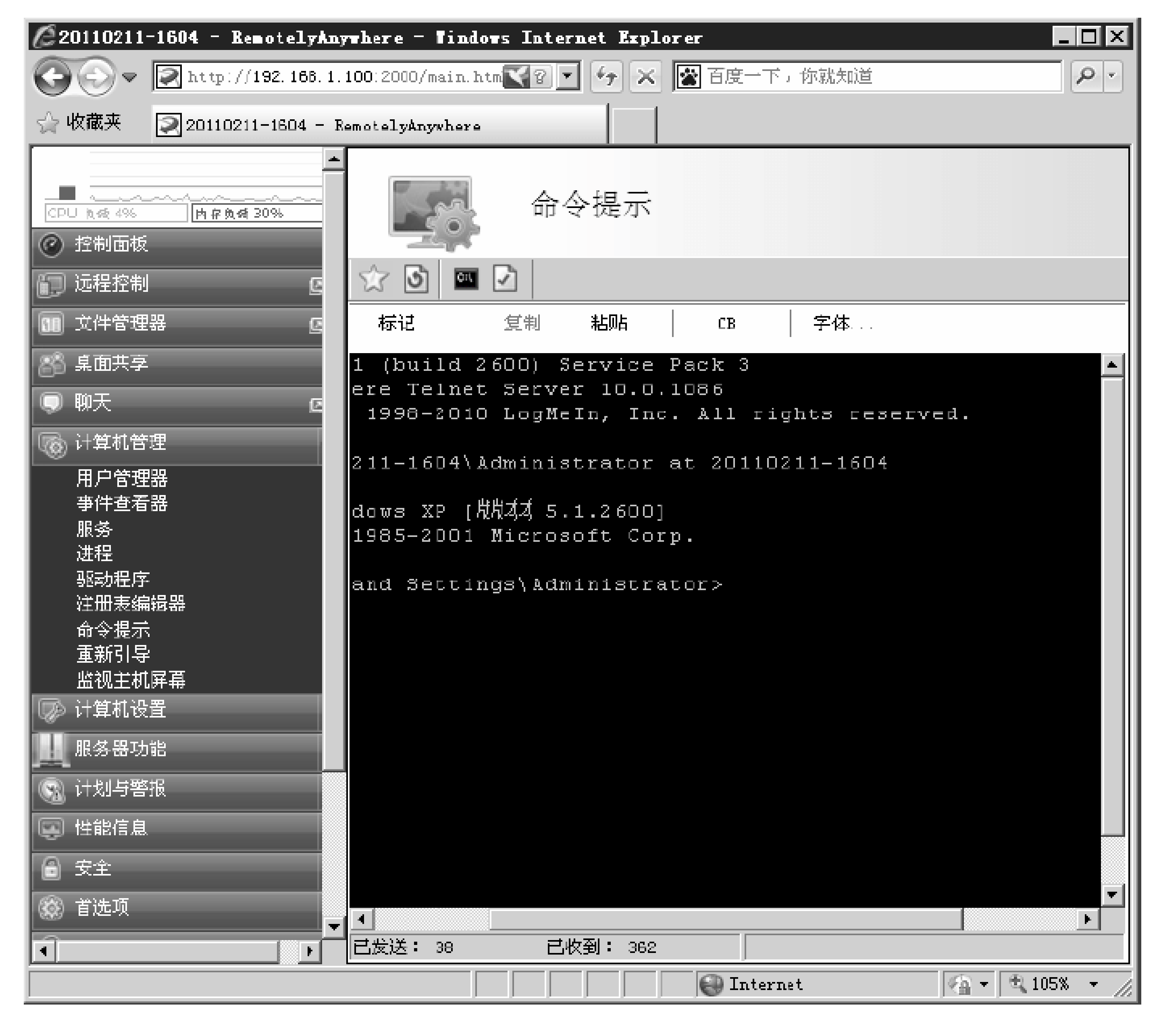


图 6-50

（7）重新引导

选择左侧列表中的【计算机管理】➢【重新引导】选项，在右侧窗格中显示了【重新引导】窗格，通过该窗格可以根据需求对远程服务器做各种引导操作，只需要单击指定的图标按钮就可以，如图 6-51 所示。



图 6-51

7. 计算机设置

有很多设置项可以通过本块内容来实现，比如环境变量、虚拟内存、系统时间、共享资源等，

下面以环境变量和虚拟内存的设置为例做简单介绍。

（1）环境变量

选择左侧列表中的【计算机设置】➢【环境变量】选项，在右侧窗格中显示了【环境变量】窗格，通过该窗格可以修改远程服务器的环境变量信息，通过单击指定环境变量选项进行调整，如图 6-52 所示。

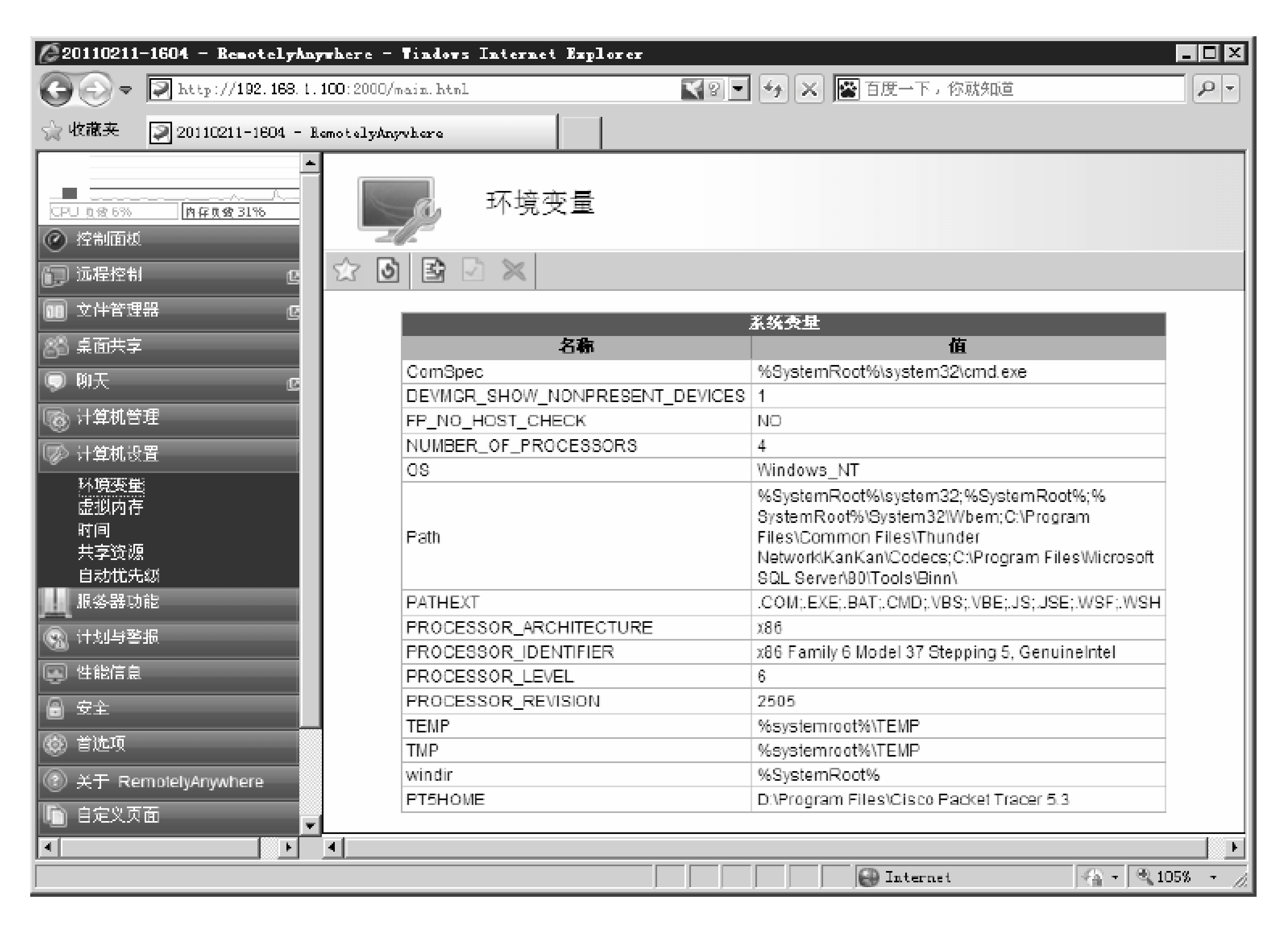


图 6-52

（2）虚拟内存

选择左侧列表中的【计算机设置】➢【虚拟内存】选项，在右侧窗格中显示了【虚拟内存】窗格，通过该窗格可以修改远程服务器的不同磁盘驱动器提供虚拟内存的数量，建议不要选择 C 盘，总量设置为物理内存的 1.5 倍，单击【应用】按钮使配置生效，如图 6-53 所示。

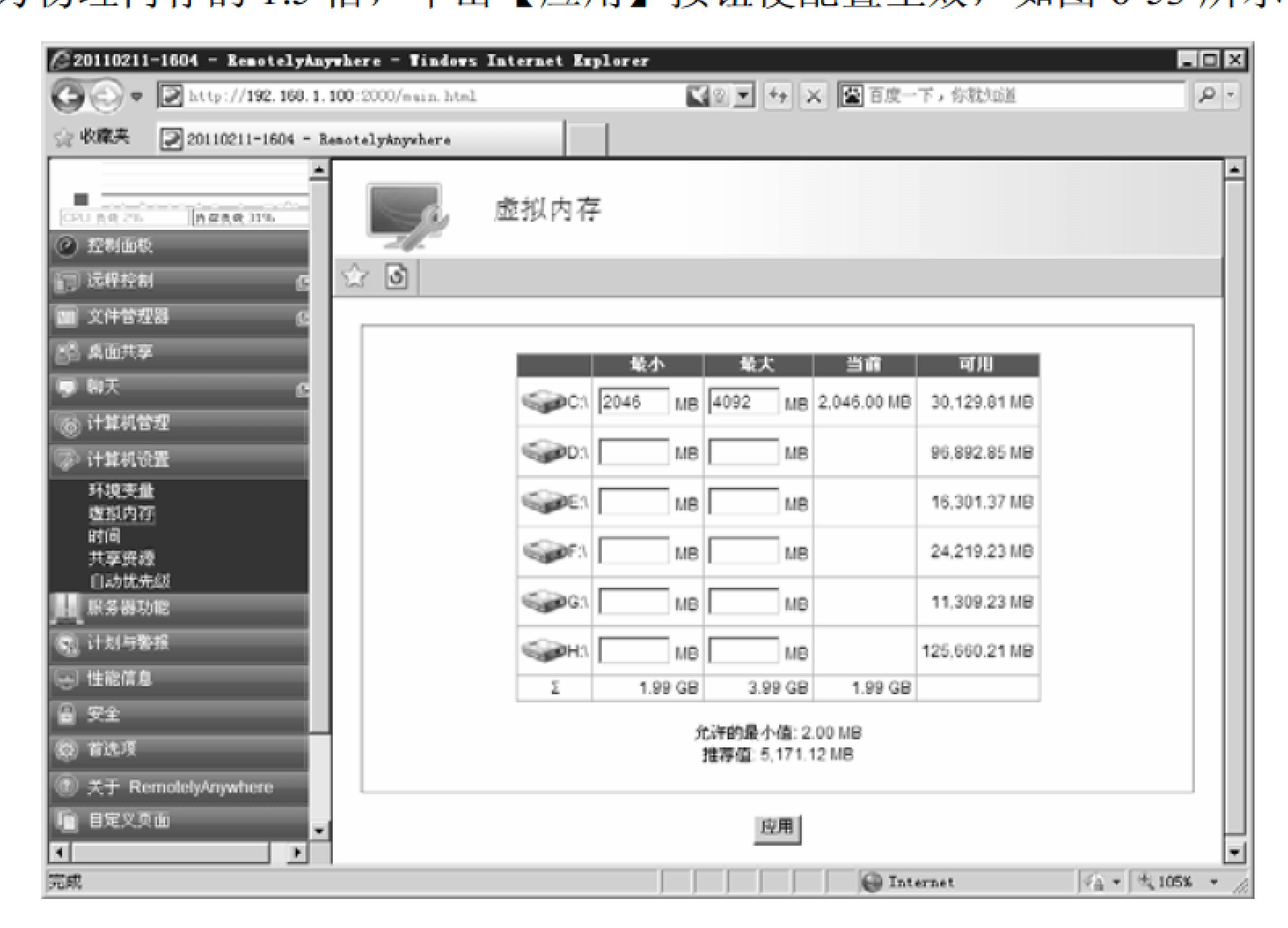


图 6-53

8. 服务器功能

通过 RemotelyAnywhere 还可以进行个别服务器的配置，比如 FTP、活动目录，如图 6-54 所示。不过一般不建议使用该功能。



图 6-54

9. 计划与警报

在左侧选项列表中选择【计划与警报】选项，该选项下有三个子选项，分别是：【系统监视】、【电子邮件警报】、【任务计划程序】。通过【系统监视】选项可以配置系统状态监视信息，还可以根据监视规则设定警报提示；通过【电子邮件警报】选项可以监视系统接收的电子邮件信息，对垃圾邮件等有安全威胁的信息提供警报提示；通过【任务计划程序】选项可以为系统配置任务计划，帮助管理员完成常规工作，如图 6-55 所示。

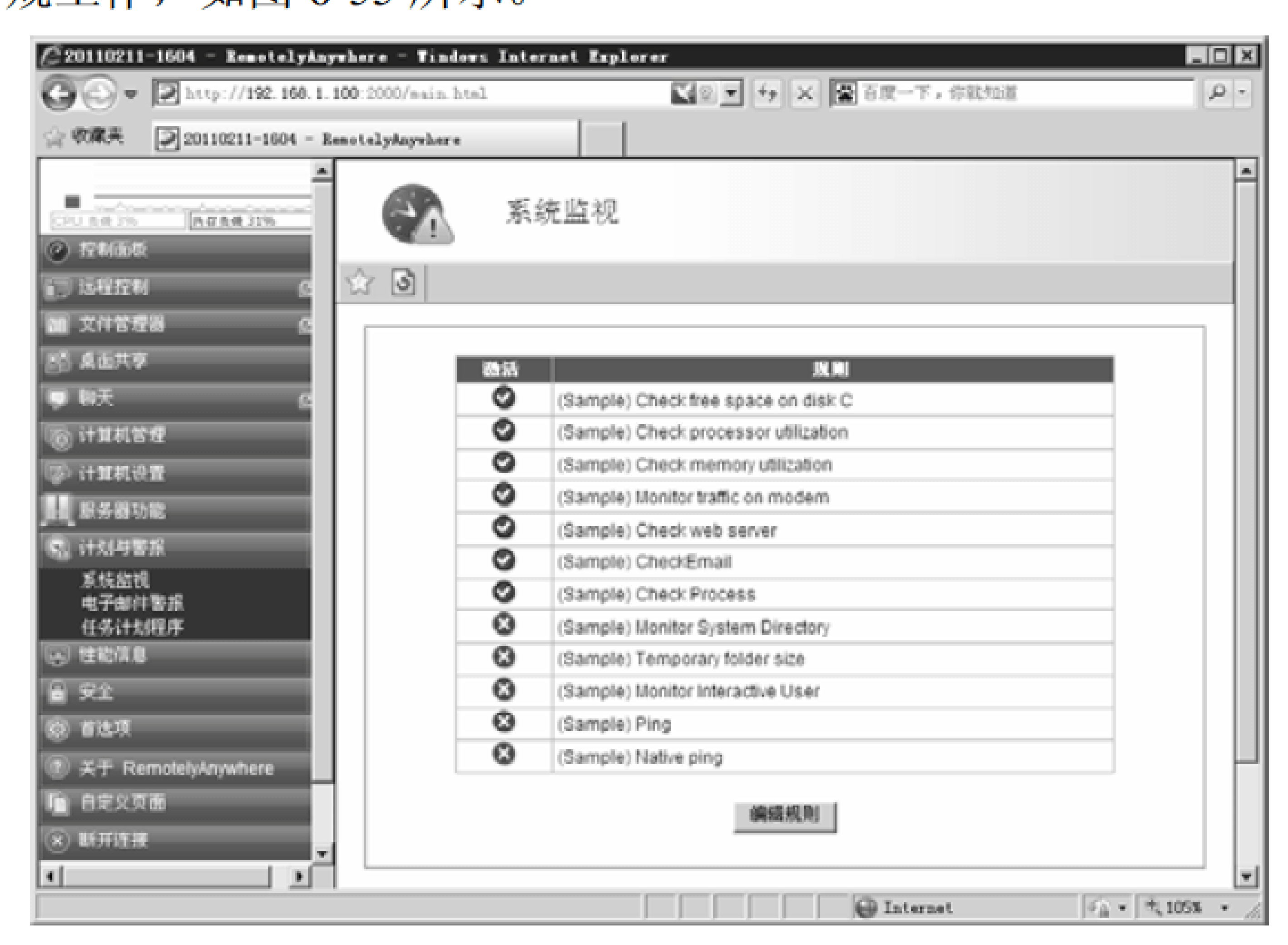


图 6-55

10. 性能信息

通过该选项可以查看远程服务器的多种性能信息，包括 CPU 负载、内存负载、磁盘空间、驱

动器与分区信息、网络负载等十几项。下面对部分性能信息进行介绍。

（1）CPU 负载

在左侧选项列表中选择【性能信息】➢【CPU 负载】选项，在右侧显示【CPU 负载】窗格，如图 6-56 所示，该窗格显示了 CPU 的使用图表，从下表中可以看到各个进程的 CPU 使用情况。



图 6-56

（2）驱动器与分区信息

在左侧选项列表中选择【性能信息】➢【驱动器与分区信息】选项，在右侧显示【驱动器与分区信息】窗格，该窗格显示了远程服务器磁盘分区情况及各个分区的状态信息。可以单击指定分区进行分区调整，如图 6-57 所示。



图 6-57

11. 安全设置

通过该选项可以为远程服务器配置安全设置，包括：访问控制、IP 地址锁定、IP 过滤、Windows 密码、SSL 设置等。下面对部分安全设置进行介绍。

（1）访问控制

在左侧选项列表中选择【安全】➢【访问控制】选项，在右侧显示【访问控制】窗格，通过该窗格可以设置部分访问控制内容，如为特定用户指定访问权限。配置完成后单击【应用】按钮使之生效，如图 6-58 所示。



图 6-58

（2）IP 地址锁定

在左侧选项列表中选择【安全】➢【IP 地址锁定】选项，在右侧显示【IP 地址锁定】窗格，通过该窗格可以对非法访问远程服务器的地址进行锁定操作，通过【拒绝服务过滤器】和【验证攻击过滤器】两项来完成配置。【拒绝服务过滤器】根据对服务器 HTTP 无效请求数进行 IP 地址锁定，【验证攻击过滤器】根据对服务器无效验证数进行 IP 地址锁定，超出阈值的按照规定时间锁定地址，如图 6-59 所示。



图 6-59

（3）IP 过滤

在左侧选项列表中选择【安全】➢【IP 过滤】选项，在右侧显示【IP 过滤】窗格，通过单击右侧窗格的【添加】按钮，可以为远程服务器添加 IP 过滤策略，选择配置好的配置文件，单击【使用配置文件】按钮，可以使该项 IP 过滤策略生效，如图 6-60 所示。

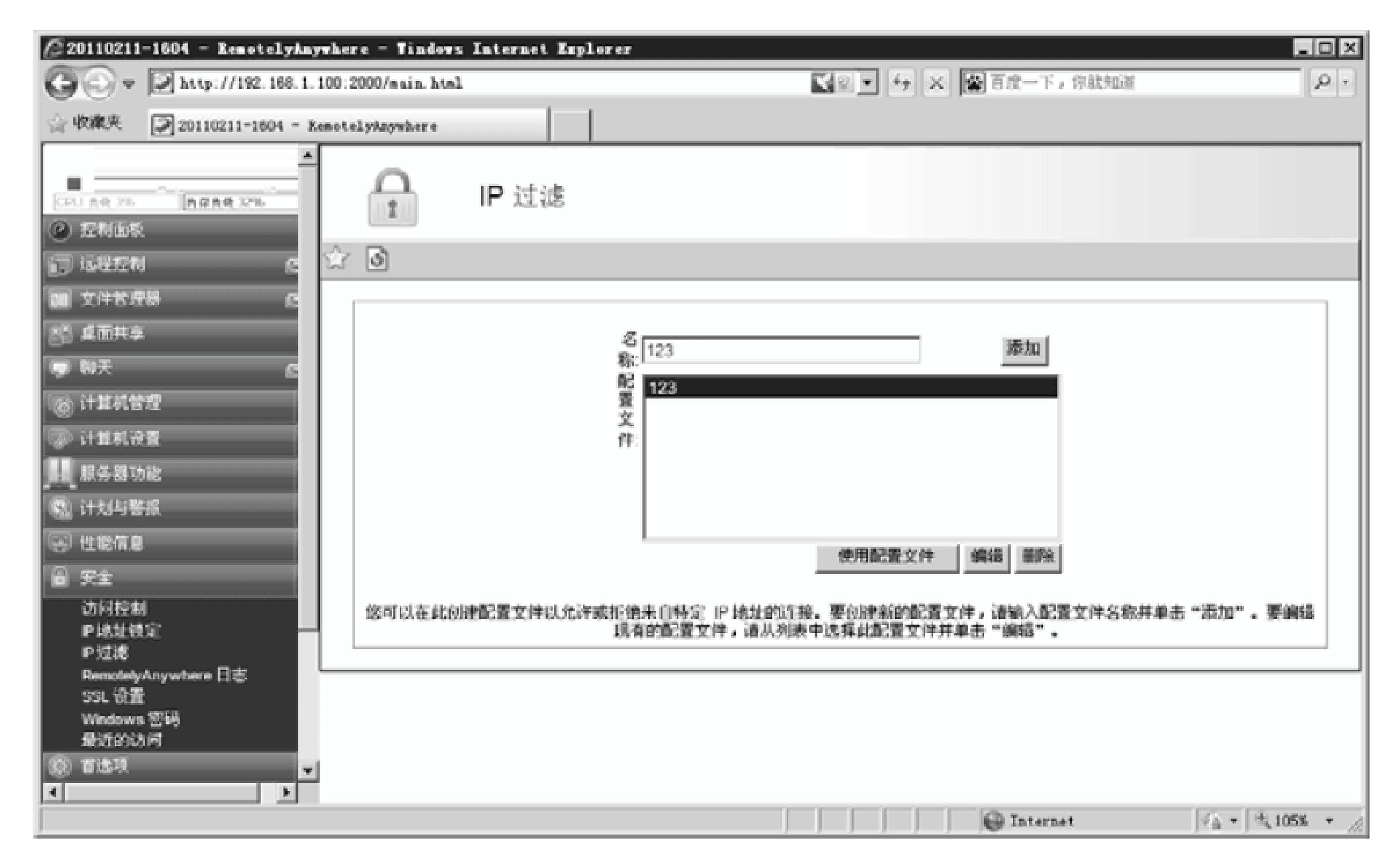


图 6-60

6.6　专家答疑

（1）远程服务器管理时，如果管理信息需要通过互联网，应当如何保证安全？

答：一部分服务器都会在企业内部使用，网络管理员访问的时候只要保证服务器主机安全，并且在网络设备上做好访问控制就可以基本保证服务器安全了。但是如果服务器在远程 IDC 机房托管，或者网络管理员在外出差办公需要连接管理内网服务器时，网络服务器管理信息会在公共互联网上传递，很容易被窃取。

这类安全问题一般可以通过需要管理端和被管服务器端进行严格认证的服务器管理程序来完成，这样普通网络用户没有有效的认证权限，就无法借此攻击服务器，不过其他合法的访问信息还是会暴露在互联网上，依然无法确保安全。

相比之下，VPN 技术是一项更好的互联网通信技术，网络管理员在进行远程服务器管理时如果跨域互联网，可以在两端使用 VPN 技术互联，然后让信息在 VPN 虚拟专用网中传输，以确保管理信息的安全加密和完整性校验。

（2）如果需要管理的远程服务器比较多，不方便记忆怎么办？

答：远程管理服务器时，服务器的地址可以配置对应的域名，域名在定义时可以定义方便记忆的名称，这样可以减少不方便记忆的麻烦。

第 7 章　网络流量监测分析

网络流量监测分析是指捕捉并分析网络中传输的数据包，通过它可以掌握网络运行状况，有效帮助网络管理人员快速准确定位故障点，快速排查网络故障，从而提高网络性能，降低网络安全风险，增大网络可用性价值，确保整个网络的持续可靠运行。

7.1　网络流量分析的意义

网络流量监测分析的主要作用是通过连续地采集网络中的数据包进行分析，帮助网络管理员深入了解网络的运行状况，发现网络中出现的问题，从而保证网络的服务质量。

通过对网络流量的分析，网络管理员可以详细地了解网络的运行状况。网络中的各种应用在运行的时候，每一个数据访问，每一个数据传输都要通过网络进行，通过分析网络数据包，可以清晰地了解应用程序的运行规律，从而帮助网络管理员更好地管理网络中的各种应用程序。同时网络中的每一个用户的网络行为也都会影响到网络中的其他用户甚至整个网络的运行。每个用户的网络行为都会产生网络流量，通过对这些流量进行分析，可以清晰地检测到每个用户的具体网络行为，从而更好地对网络用户进行管理。

通过对网络流量的分析，网络管理员可以及时发现网络出现的问题。任何的网络异常，比如网络用户的计算机感染了蠕虫病毒、中了后门程序等，都会产生异常的数据包，通过对数据包的长期分析就能及时发现网络用户的异常行为，从而提高解决问题的效率。

网络流量分析建立在深入了解网络的基础之上，通过对网络数据包的深入分析，及时发现网络流量中的异常数据包，可以帮助网络管理员及时解决网络故障，提高网络运行效率。

7.2　主流产品技术介绍

要进行网络流量分析监测，除了要掌握扎实的网络基础知识外，还必须使用网络数据包嗅探工具。通过网络数据包嗅探工具捕捉网络中的数据包，然后对其进行分析。现在，主流的网络数据包嗅探工具有 Sniffer Pro 网络嗅探工具和科来网络分析系统等。

7.2.1　Sniffer Pro 网络嗅探工具概述

Sniffer Pro 网络嗅探工具是目前最为流行的网络嗅探工具之一。Sniffer 的主要功能是捕获网络

数据，在大量的数据包中找到自己关心的数据包，然后分析解决问题。通过使用 Sniffer 嗅探工具，网络管理员可以判断在某个时间网络中的某个主机使用网络的具体行为，比如该主机接收了多少数据包、发送了多少数据包、正在访问什么网站等信息，也可以判断整体网络的运行情况，比如当前网络中运行了什么协议、哪个协议占用带宽过大、现在网络带宽使用率是多少等。因此，Sniffer 可以帮助管理员解决很多隐形的网络故障。

选择 Sniffer 的安装位置非常重要，因为 Sniffer 只能捕捉到它所监听的网卡接收到的数据包，因此在不同的网络拓扑环境中，Sniffer 的安装位置不同。现在的网卡都有一个数据包识别功能，就是当网卡接收到一个数据包的时候，会智能判断该数据包是不是发送给自己，只有当判定该数据包是发给自己的时候才会接收该数据包。如果要实现 Sniffer 监听网络数据包，必须将网卡处于“混杂模式”，所谓混杂模式就是网卡可以接收所有发送给自己的数据包，不考虑该数据包中的目的地址是不是自己。下面详细讲解在不同的网络环境中，Sniffer 的安装位置。

集线器所连接的网络被称之为共享式以太网，共享式以太网中的数据通信依靠广播来完成，因此只要将主机的网卡设为混杂模式，也就意味着网络中的任何一个主机网卡都可以接收到网络中的所有数据包。在安装 Sniffer Pro 的计算机上，计算机的网卡会自动变成混杂模式。在集线器所连接的以太网中，Sniffer 的安装位置如图 7-1 所示。

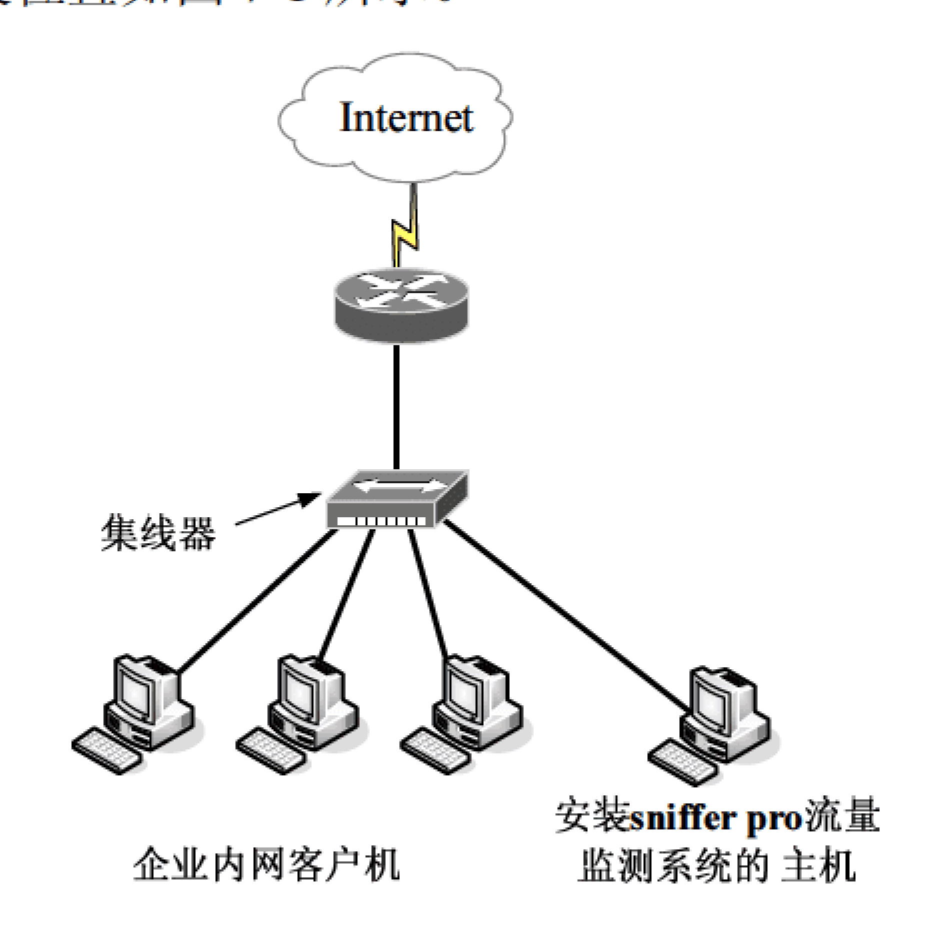


图 7-1

交换机所连接的网络被称之为交换式以太网，交换式以太网中的数据通信是点到点通信，网络中的每个主机只接收发送给自己的数据包。在交换式以太网中，要想让 Sniffer 能够监听到网络中所有的数据包，有以下两种方法。

（1）在以太网中，如果使用的是网管级交换机连接路由器去连接互联网，要想让 Sniffer 监听到内部局域网和外部互联网的通信情况，可以在网管级交换机上配置端口镜像，并将网络设备的出口设置为目的端口，然后将 Sniffer 安装在连接在该端口的计算机上，就可以监听到整个网络，Sniffer 的安装位置如图 7-2 所示。

镜像一般是将符合制定规则的报文复制到镜像目的端口。镜像目的端口一般会接入数据检测设备，用户利用这些设备对镜像过来的报文进行分析，从而进行网络监控和故障排除等。所谓端口镜像就是把交换机一个或多个端口（VLAN）的数据镜像到一个或多个端口的方法。一般情况下，

在这种以太网中为了实现对整个网络数据的监听，将交换机连接路由器（公司连接互联网用的路由器）的端口映射为 Sniffer 所在计算机连接的端口。需要注意的是，不一样的交换机设置方法不同，这里简单介绍下 Cisco 交换机端口镜像设置方法。

```
Router#configure terminal
//进入全局配置模式
Router(config)#monitor session 2 source interface g1/0/1
//指定端口镜像进程和侦听源端口（g1/0/1）
Router(config)#monitor session 2 destination g1/0/2
//指定端口镜像进程和侦听目标端口（g1/0/2）
Sniffer 的安装位置如下图。
```

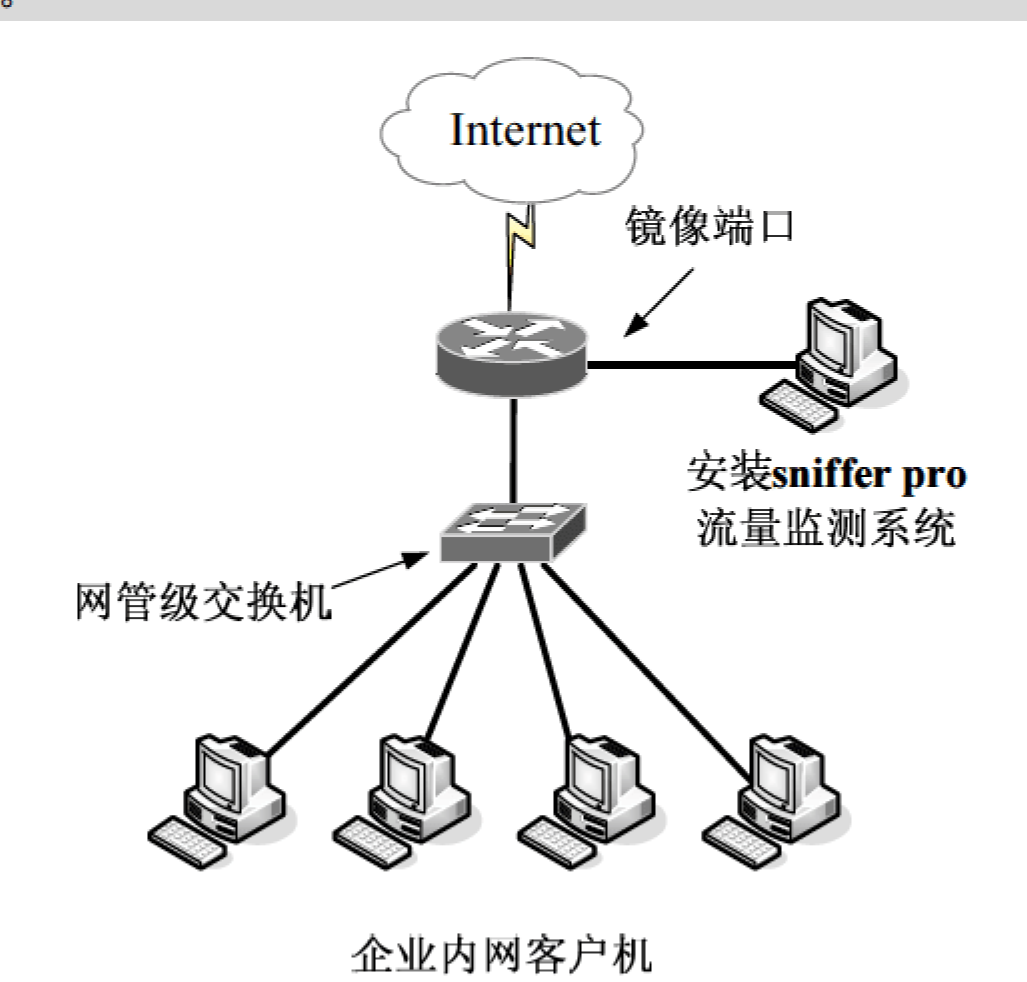


图 7-2

（2）在以太网中，如果使用的是交换机连接代理服务器连接以太网的方式，则在这种网络拓扑结构中，内部局域网所有的数据包，可以将 Sniffer 安装在代理服务器（代理内部局域网访问互联网的主机）上。Sniffer 的安装位置如图 7-3 所示。

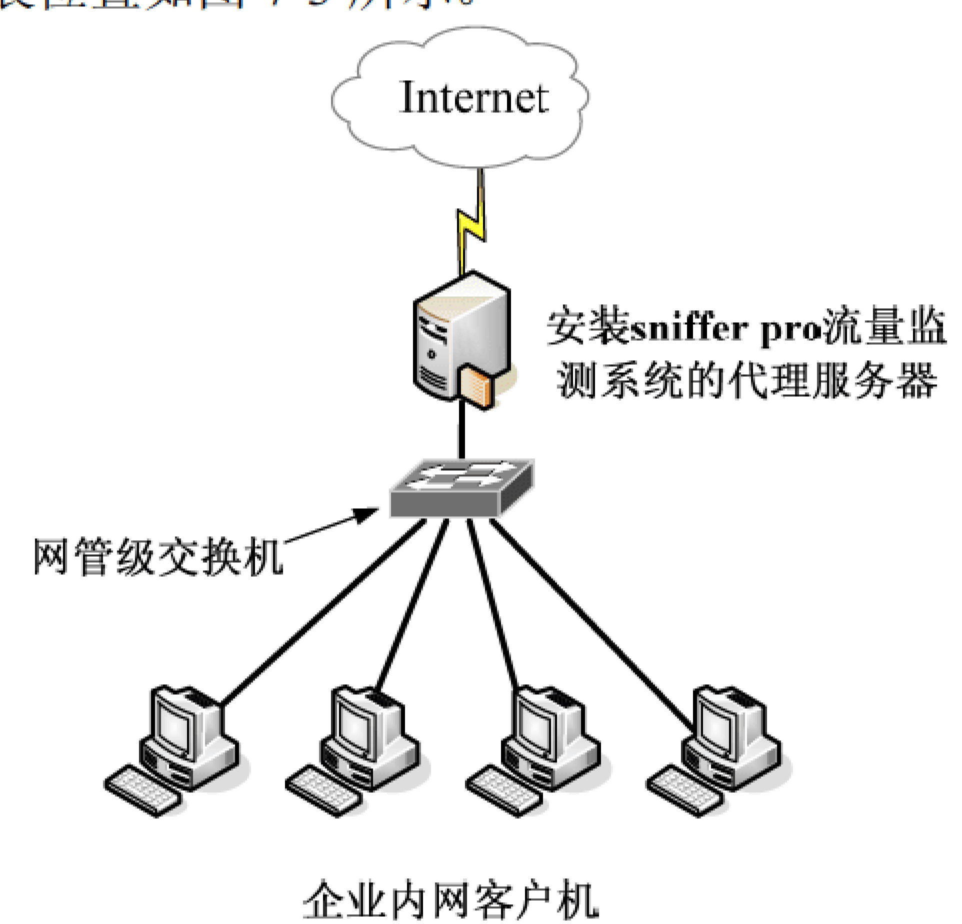


图 7-3

7.2.2 科来网络分析系统概况

科来网络分析系统是一个集数据包采集、解码、协议分析、统计、图表、报表等多种功能为一体的综合网络分析平台。它可以帮助网络管理员排查网络安全隐患、网络流量监控、定位网络故障。

与 Sniffer Pro 嗅探工具不同，科来网络分析系统是由中国人自主研发，并拥有全部知识产权的网络分析产品。它为网络管理工作提供了全面可靠的数据依据，可以帮助用户排查网络故障、规避网络风险、提升网络性能、提高故障处理能力、减少故障损失并降低管理成本，所以，科来网络分析系统是网络管理中的必备产品。

科来网络分析系统能够让网络管理者在遇到各种网络问题的时候，轻松找到解决办法，对网络中监测到的数据进行分析、诊断，从而帮助网络管理人员及时排除网络故障，规避网络安全风险，提高网络性能。

使用科来网络分析系统，网络管理者不用再担心遇到网络故障无法解决，因为科来网络分析系统成熟的数据包分析机制可以帮助企业把网络故障和安全风险降到最低，网络性能会逐步得到提升。总体上来说，科来网络分析系统可以帮助管理员快速的查找和排除网络故障，及时地解决网络瓶颈提升网络性能，并且能够分析各种网络协议，从而更好的管理资源，提高网络应用质量。

科来网络分析系统整合了行业领先的专家分析技术，对当前复杂的网络提供精确分析，在网络安全、网络性能、网络故障方面提供最全面和最深入的数据依据，是企业、政府、学校等网络管理所需要的关键性产品。

7.3 项目实施 1：科来网络分析系统的安装与使用

科来网络分析系统和 Sniffer Pro 一样，安装位置特别重要，应该安装在网络的节点处以便能够捕获到需要的数据包，可根据上文中 Sniffer Pro 的讲解选择科来网络分析系统的安装位置。下面介绍科来网络分析系统的安装与使用方法。

7.3.1 安装科来网络分析系统

安装科来网络分析系统的具体操作步骤如下。

01 双击科来网络分析系统安装文件，弹出【欢迎您使用科来网络分析系统 2010 技术交流版安装程序】对话框，单击【下一步】按钮，如图 7-4 所示。



图 7-4

02 弹出【使用许可协议】对话框，选择【我接受本协议】单选按钮，单击【下一步】按钮，如图 7-5 所示。

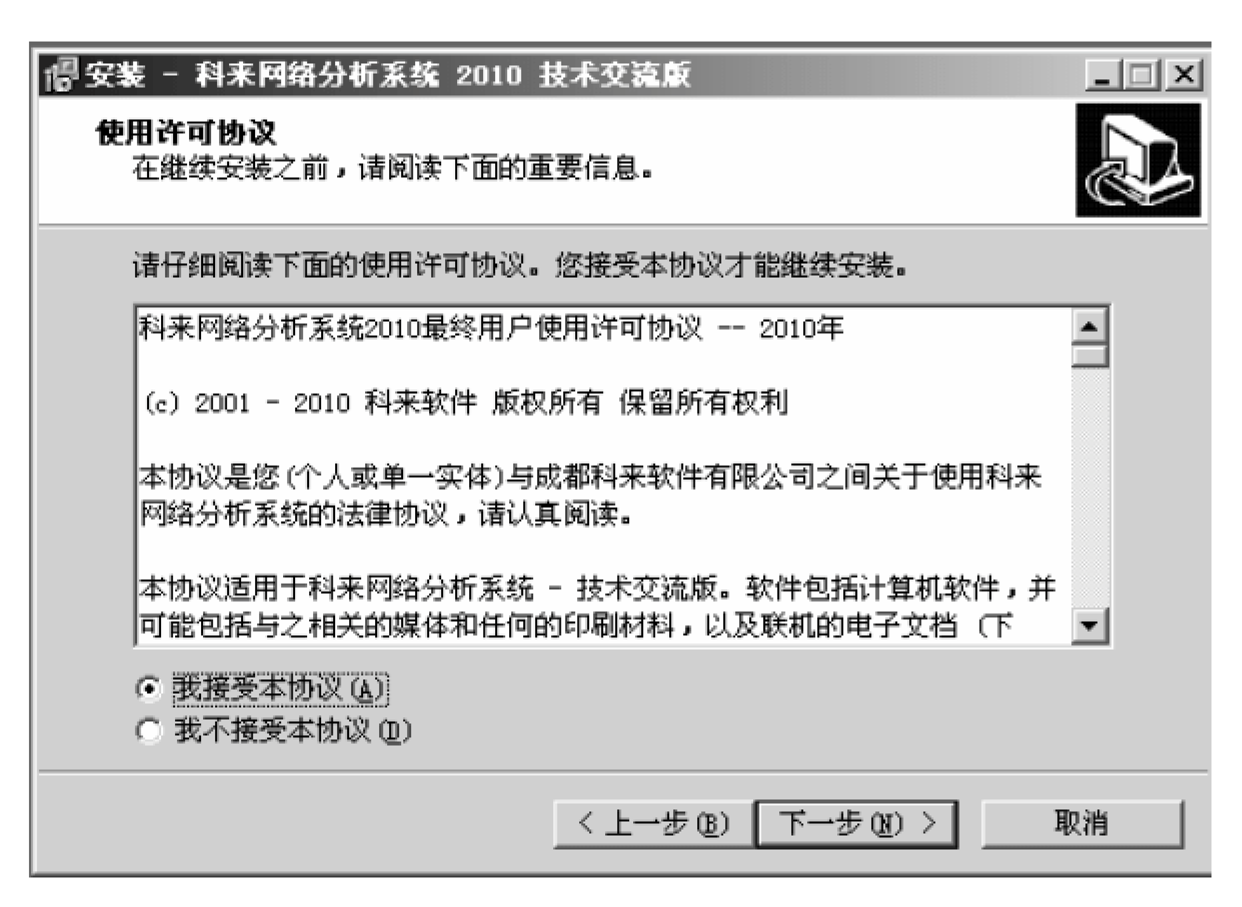


图 7-5

03 弹出【信息】对话框，显示科来网络分析系统更新信息，单击【下一步】按钮，如图 7-6 所示。

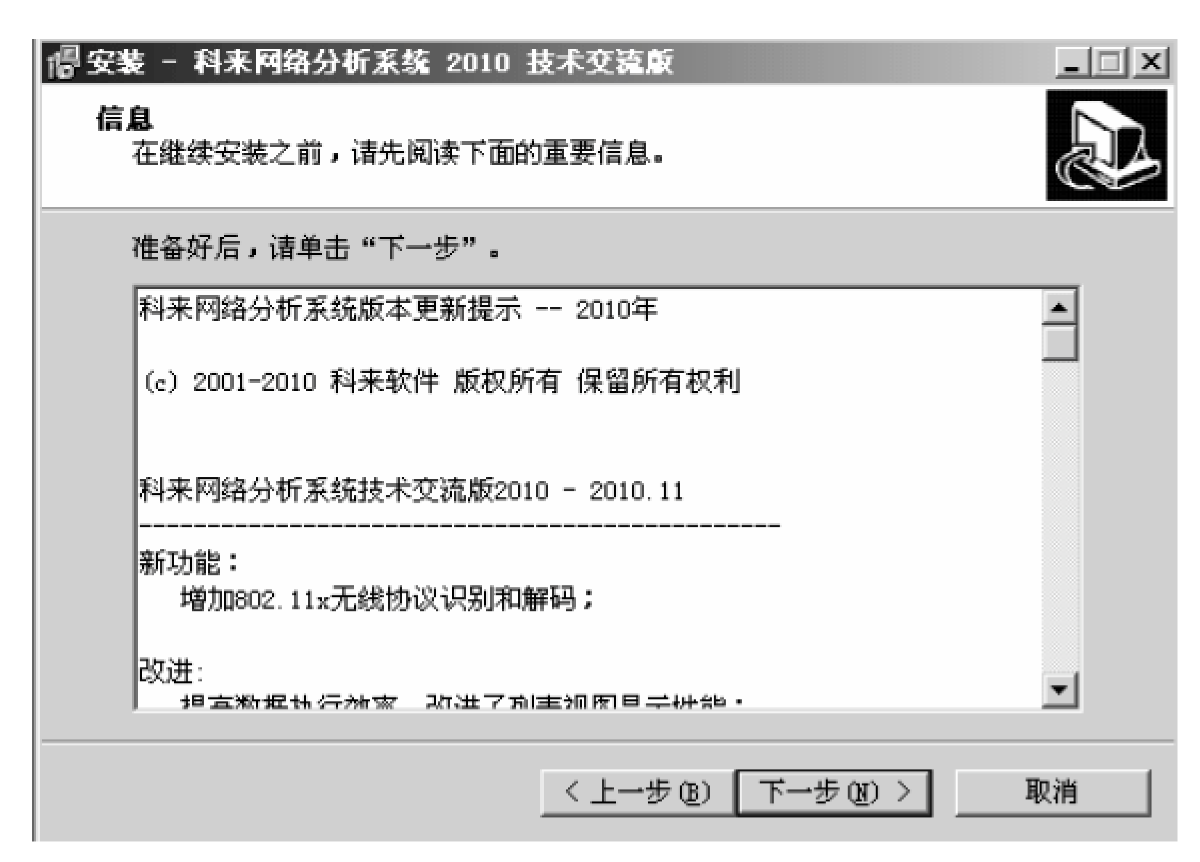


图 7-6

04 弹出【选择目标文件夹】对话框，可以单击【浏览】按钮自定义安装路径，本实例采用默认路径，单击【下一步】按钮，如图 7-7 所示。

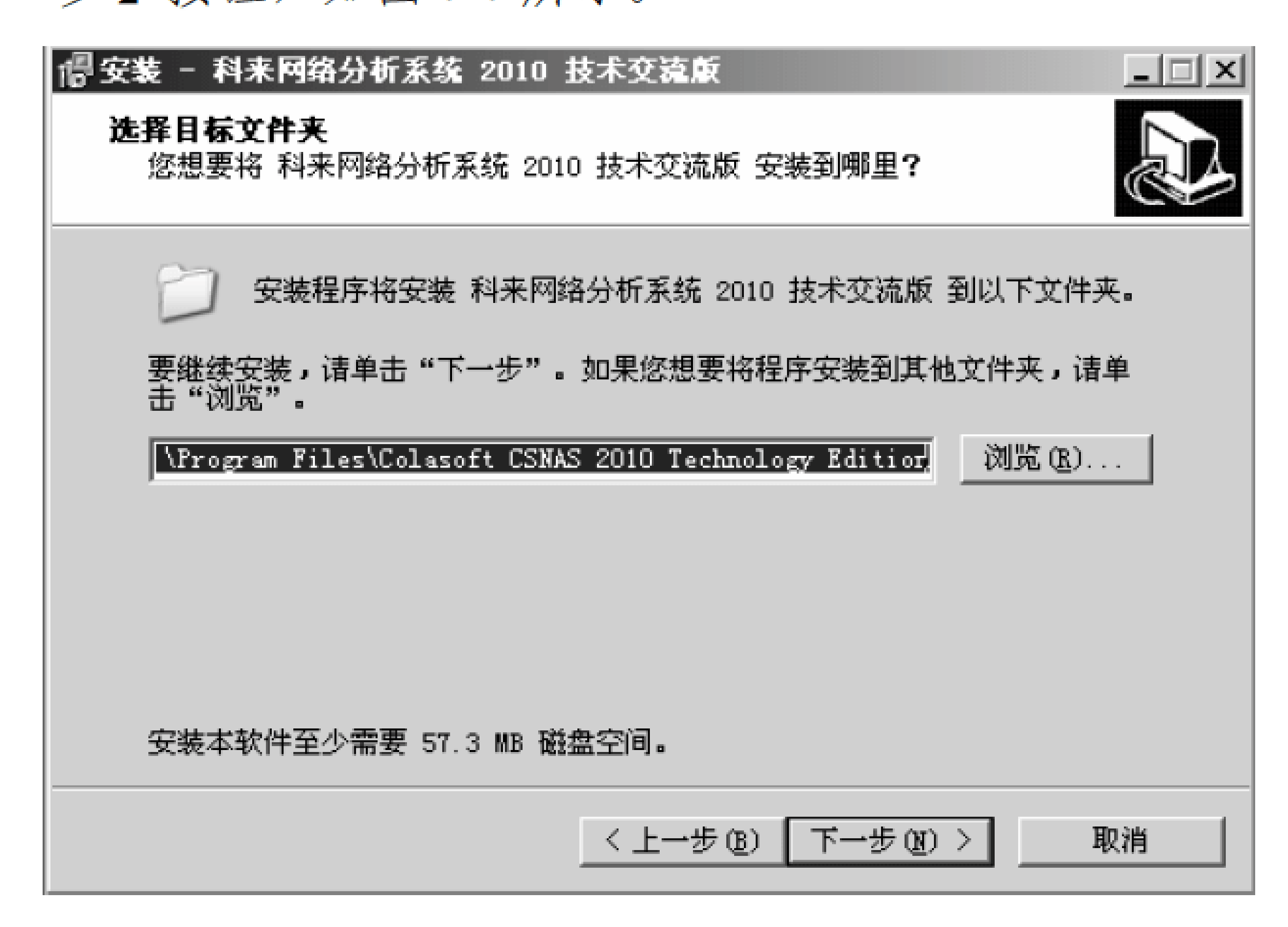


图 7-7

05 弹出【选择组件】对话框，默认选择安装所有组件，单击【下一步】按钮，继续安装科来网络分析系统，如图 7-8 所示。

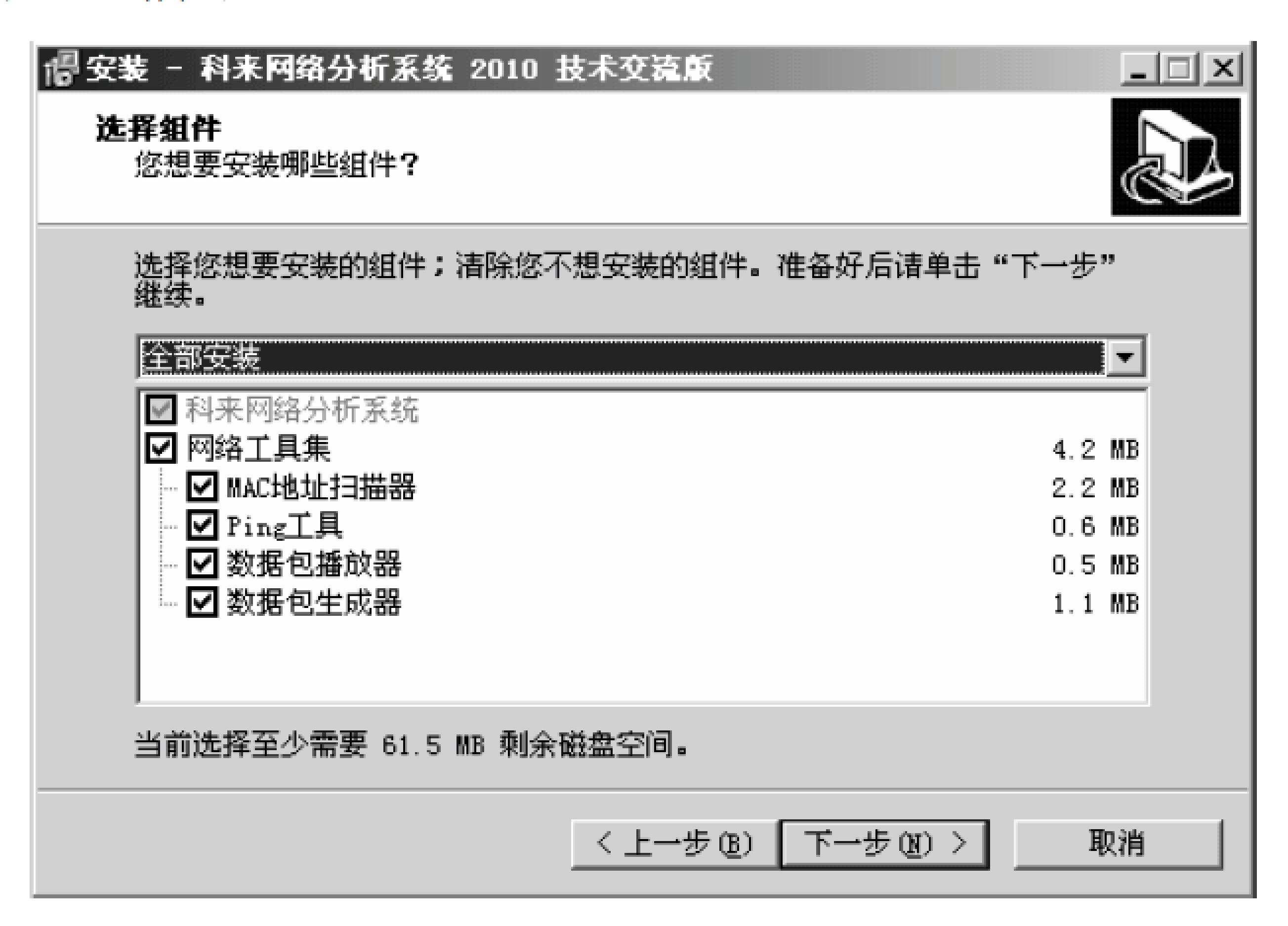


图 7-8

06 弹出【选择开始菜单文件夹】对话框，可以单击【浏览】按钮自定义科来网络分析系统的快捷方式安装路径，单击【下一步】按钮，如图 7-9 所示。

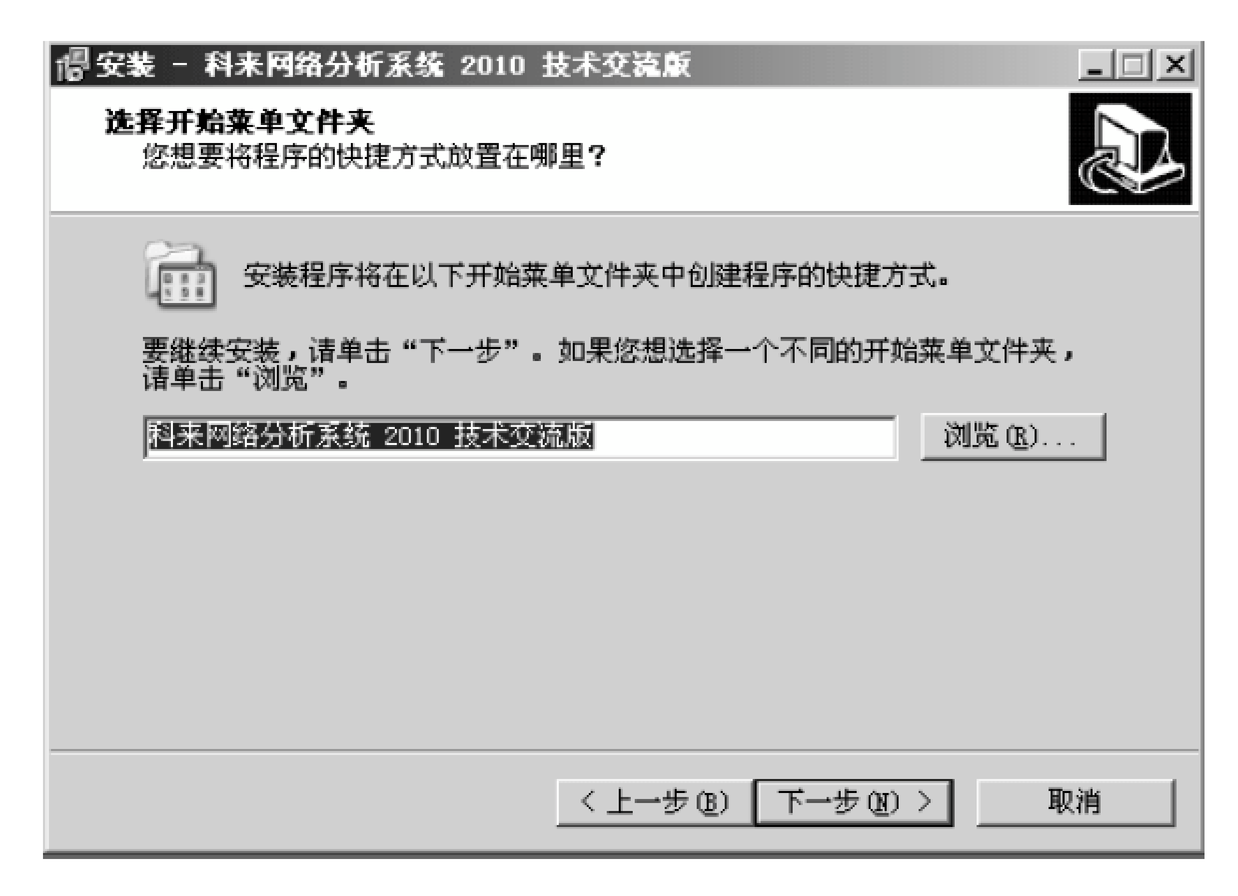


图 7-9

07 弹出【选择附加任务】对话框，选择【创建桌面图标】和【创建快速启动图标】复选框，单击【下一步】按钮，如图 7-10 所示。

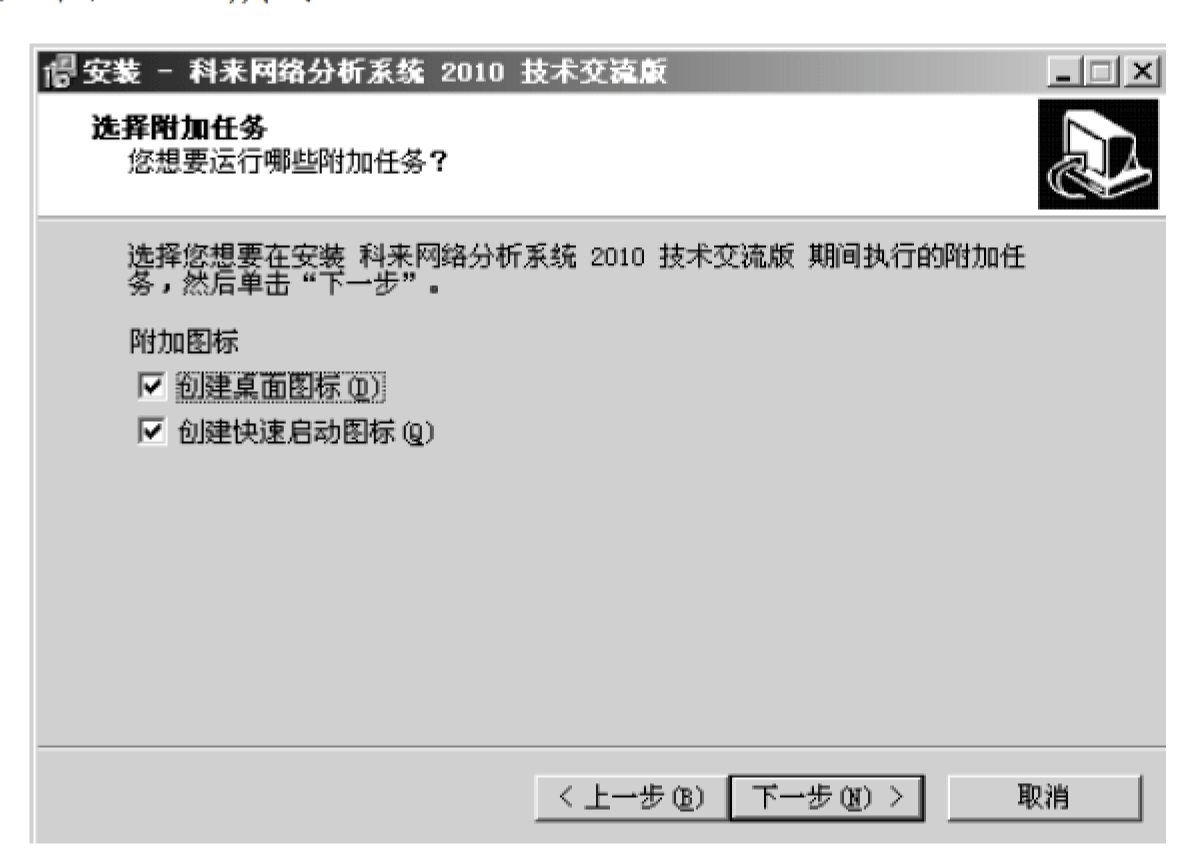


图 7-10

08 弹出【准备安装】对话框，显示了科来网络分析系统的安装信息，确认无误后，单击【安装】按钮，如图 7-11 所示。

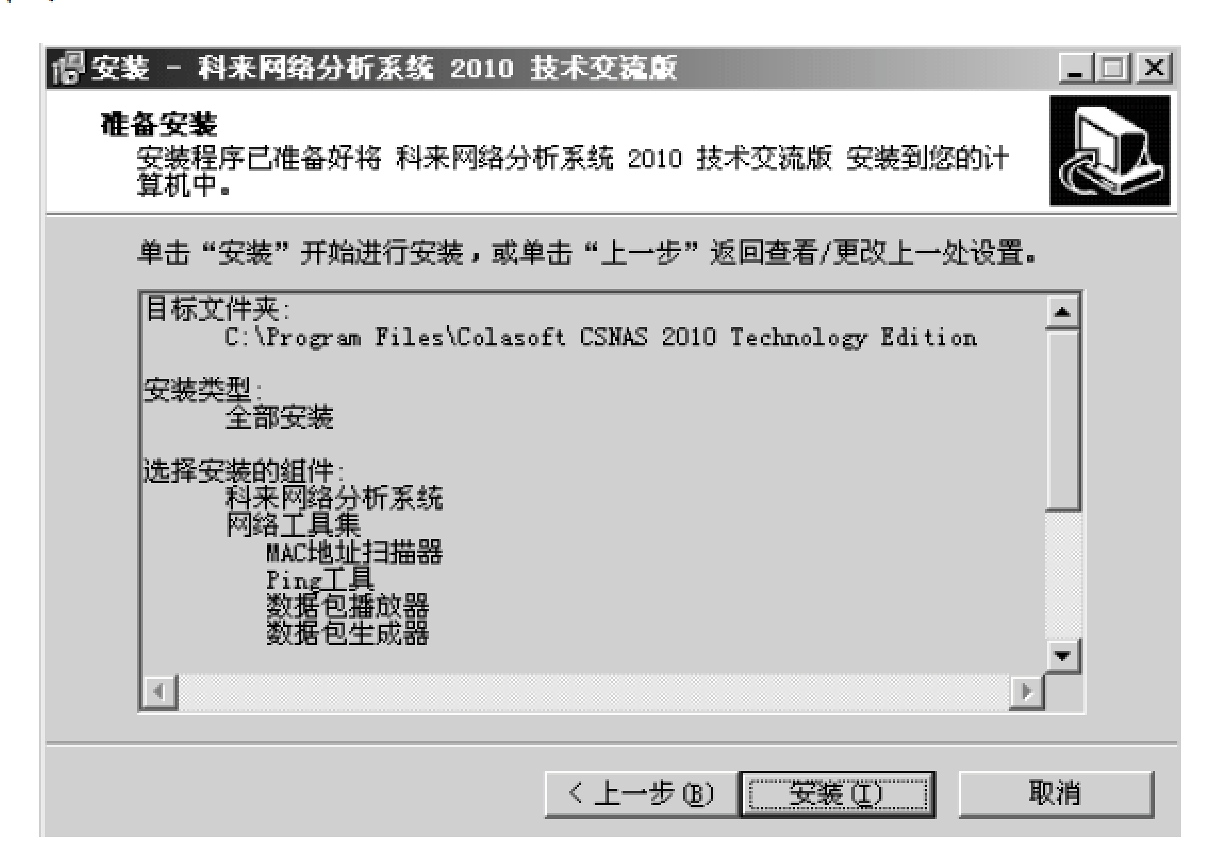


图 7-11

09 科来网络分析系统安装正在继续，并显示安装进度，如图 7-12 所示。



图 7-12

10 安装的过程中会弹出【信息】对话框，显示科来网络分析系统信息，单击【下一步】按钮，如图 7-13 所示。



图 7-13

11 单击【完成】按钮，结束科来网络分析系统的安装，如图 7-14 所示。



图 7-14

12 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分析系统 2010 技术交流版】菜单命令，打开科来网络分析系统。在【用户名】和【公司】文本框中分别输入用户名和公司信息，本实例中输入用户名为“sushi”，公司为“howin”，在【序列号】文本框中输入科来网络分析系统的序列号，序列号可以通过单击【点击这里获取序列号】超链接在线获得，单击【下一步】按钮，如图 7-15 所示。



图 7-15

13 弹出【请阅读以下重要信息】对话框，在其中显示了科来网络分析信息激活信息，单击【下一步】按钮，激活科来网络分析系统，如图 7-16 所示。

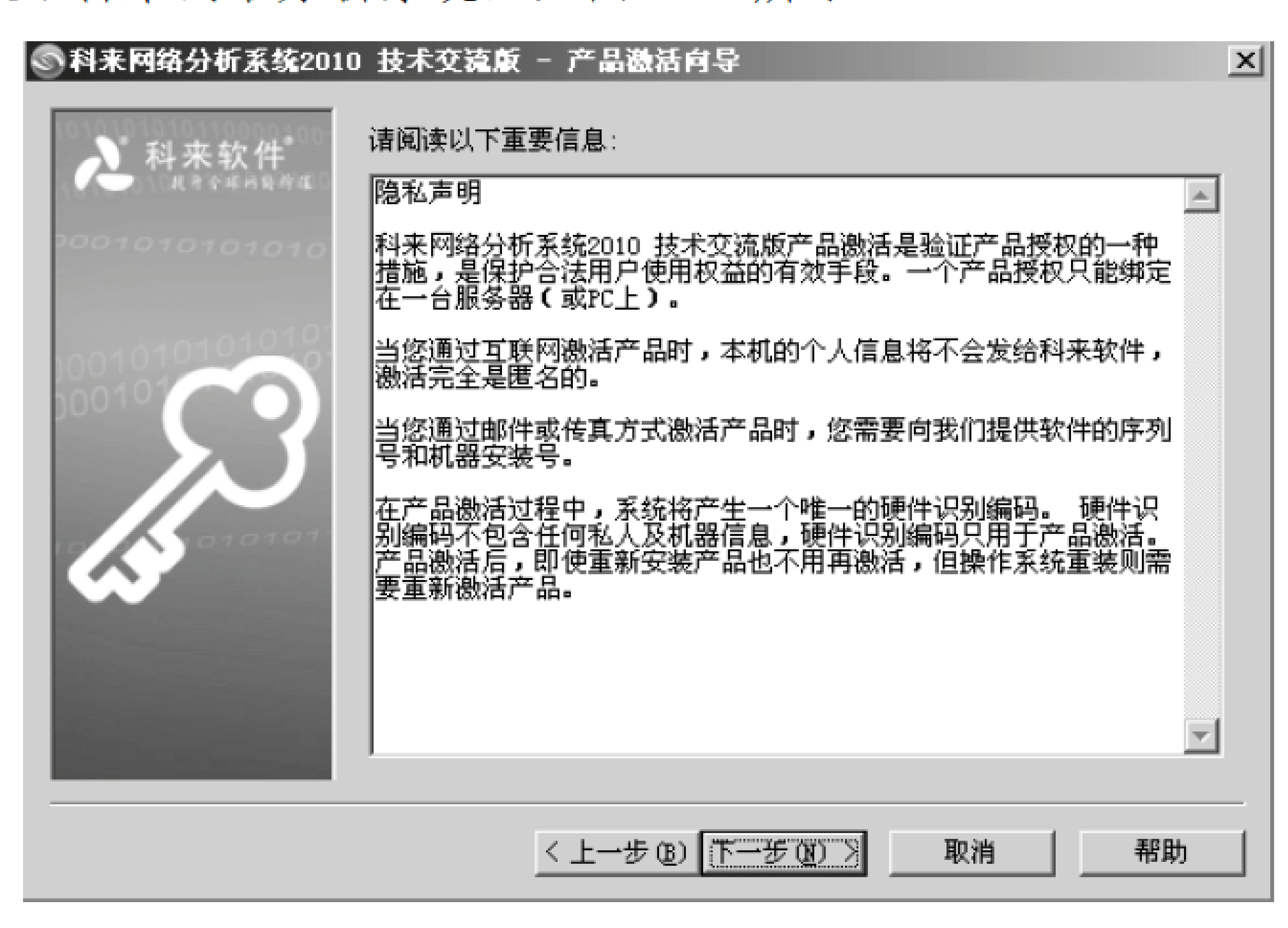


图 7-16

14 科来网络分析系统激活成功，单击【完成】按钮，如图 7-17 所示。



图 7-17

15 完成激活后，自动打开科来网络分析系统程序主界面，至此科来网络分析系统安装并激活完成，如图 7-18 所示。



图 7-18

7.3.2 设置过滤器

默认情况下，科来网络分析系统捕捉网卡监听到的所有数据包，由于每次捕捉到的数据包量比较大，不利于提高分析效率。而过滤器就是对捕捉到的数据包进行过滤，通过设置数据包过滤器可以减少捕捉到的数据包的数量，减少数据包分析时间，提高数据包分析效率，从而加快解决网络故障的速度。

设置过滤器的具体操作步骤如下。

01 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分析系统 2010 技术交流版】菜单命令，打开科来网络分析系统，选择监听网卡【本地连接】复选框，单击右侧【设置捕捉过滤器】选项，如图 7-19 所示。



图 7-19

02 弹出【过滤】对话框，默认情况下没有设置过滤器，则监听所有数据包，如图 7-20 所示。

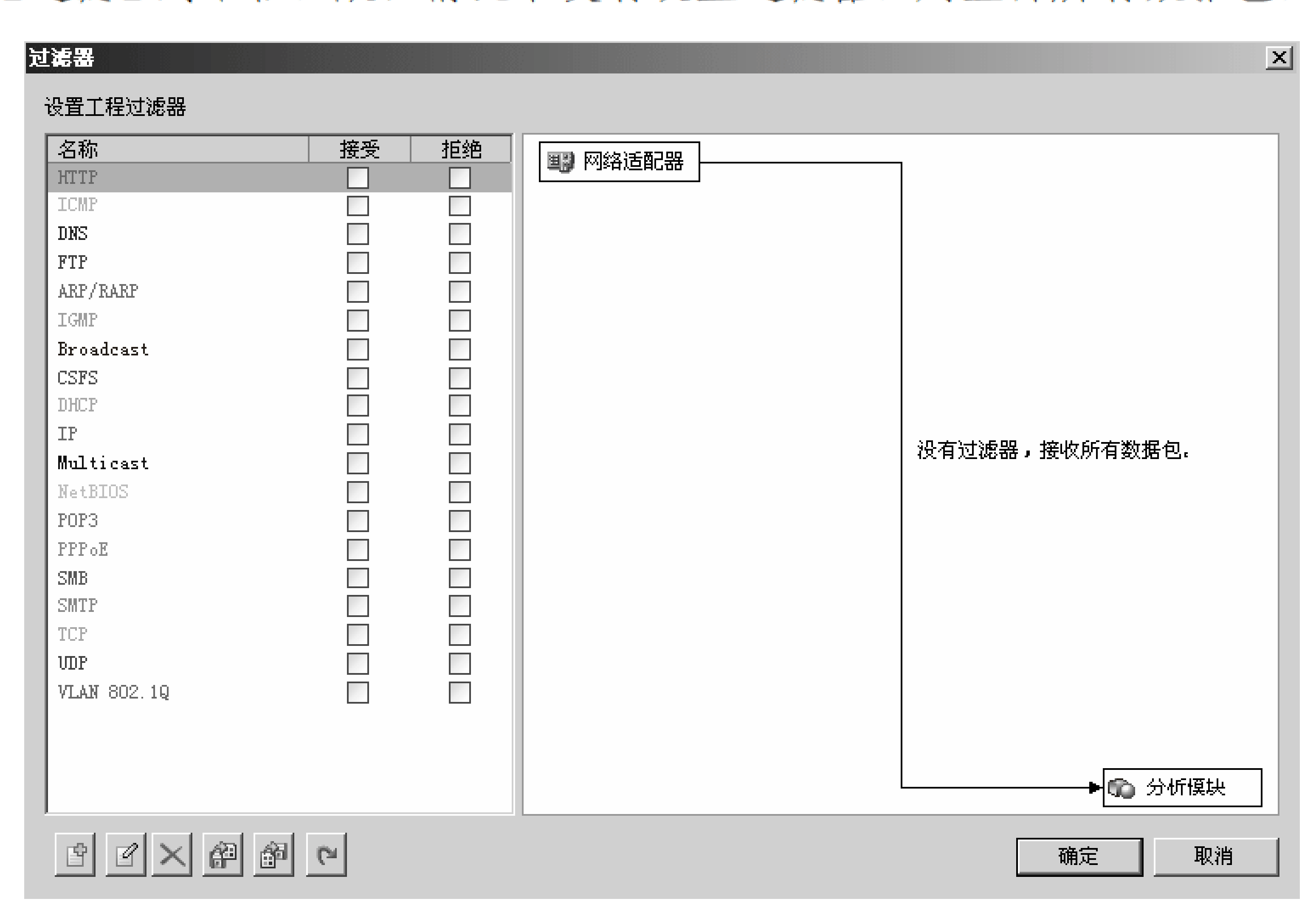


图 7-20

03 选择【ARP/RARP】协议、【接受】复选框，表明要捕捉关于 ARP/RARP 协议的数据包，单击下方的按钮，如图 7-21 所示。

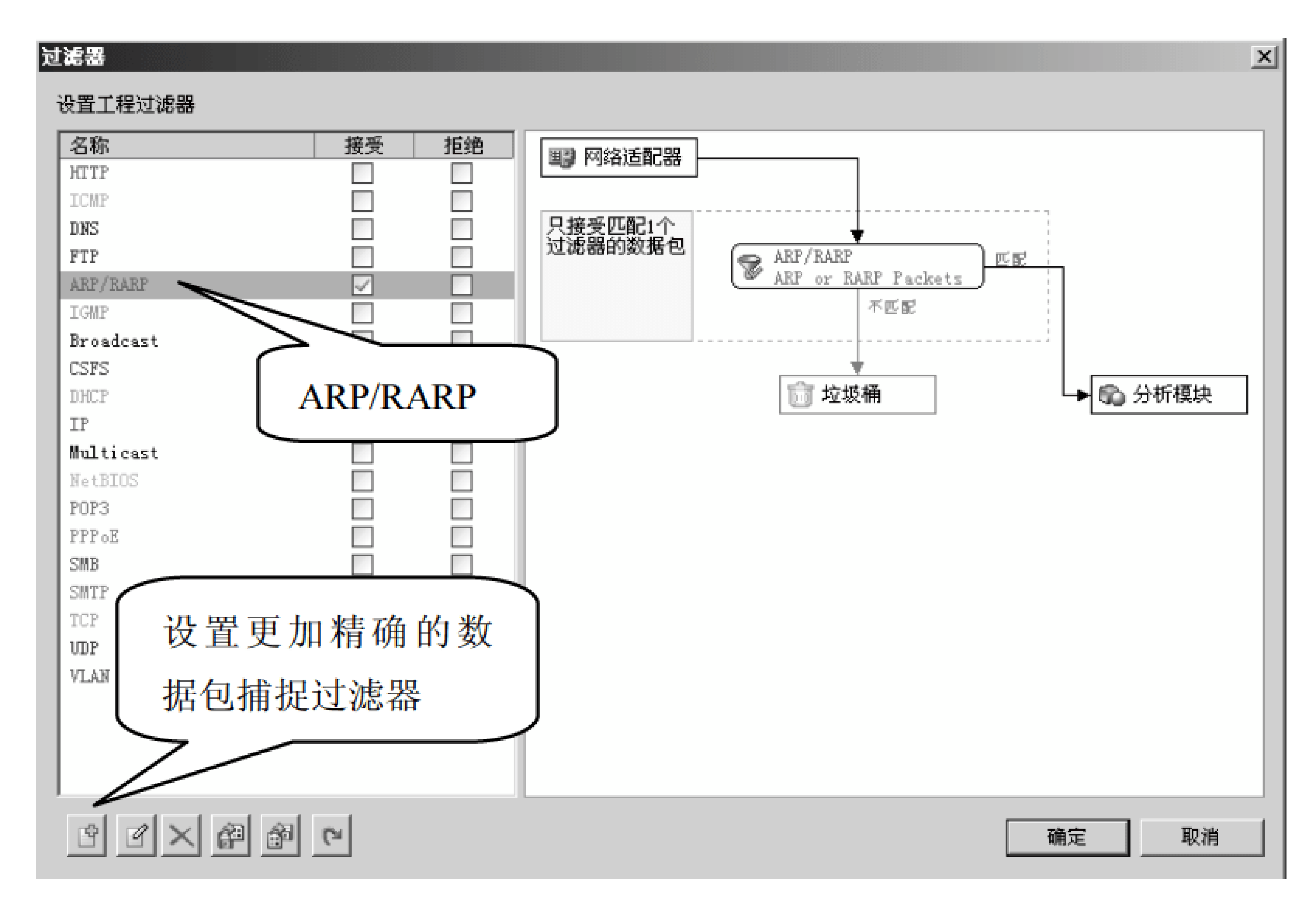


图 7-21

04 弹出【数据包过滤器】对话框，在其中设置更加精确的数据包捕捉过滤器。在【名字】文本框中输入过滤器的名称“过滤 1”，选择【地址规则】单选框，在【地址 1】下拉列表中选择【IP 地址】选项，输入【IP 地址】为“172.16.4.1”，在【地址 2】下拉列表中选择【任意地址】选项，在【方向】下拉列表中选择【地址 1<->2】菜单选项，表明只捕捉源 IP 为 172.16.4.1 的数据包，单击【确定】按钮，如图 7-22 所示。

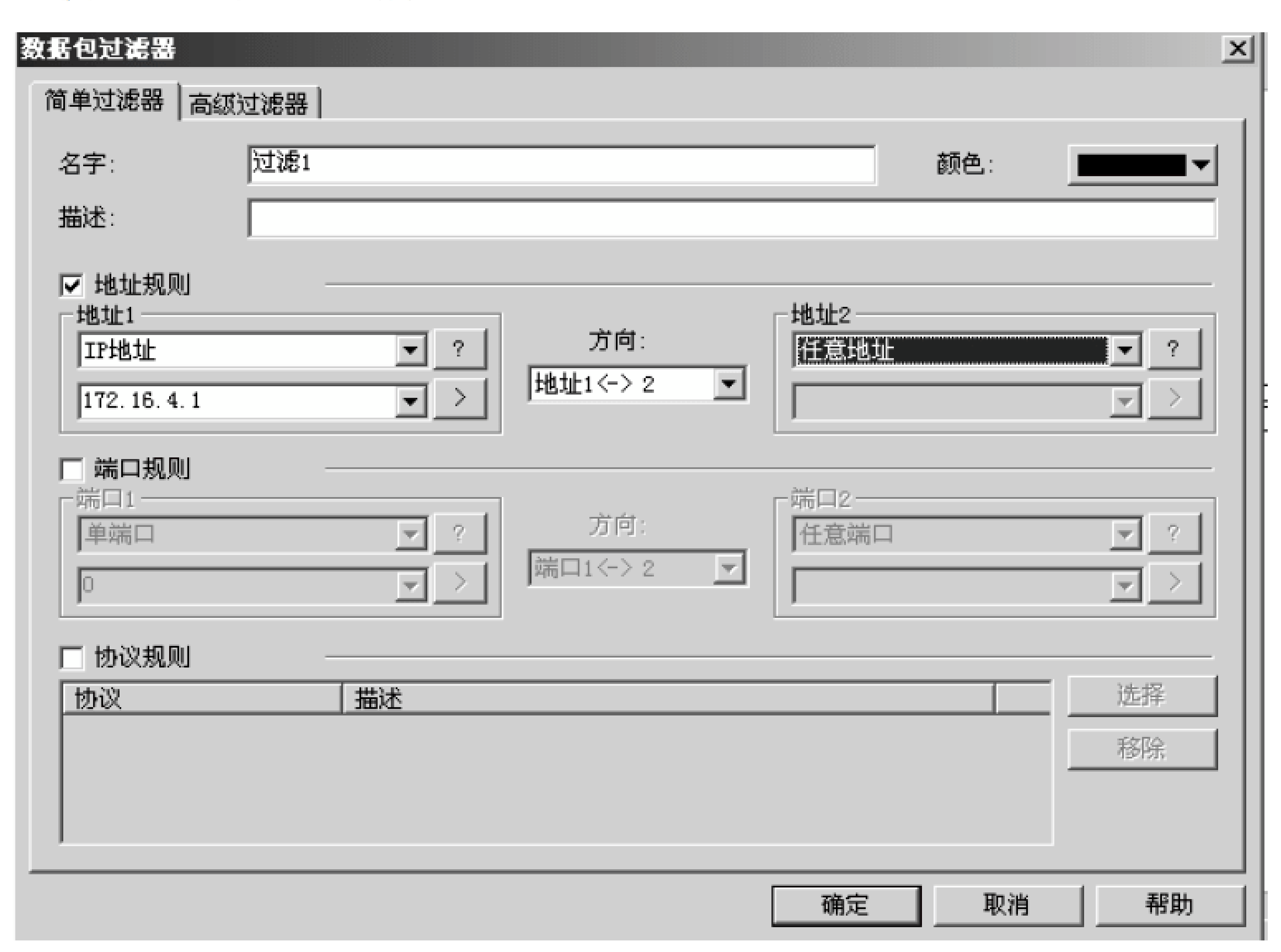


图 7-22

05 返回【过滤器】对话框，选择【过滤 1】复选框，表明使用【过滤 1】过滤器进行数据包过滤，单击【确定】按钮，如图 7-23 所示。

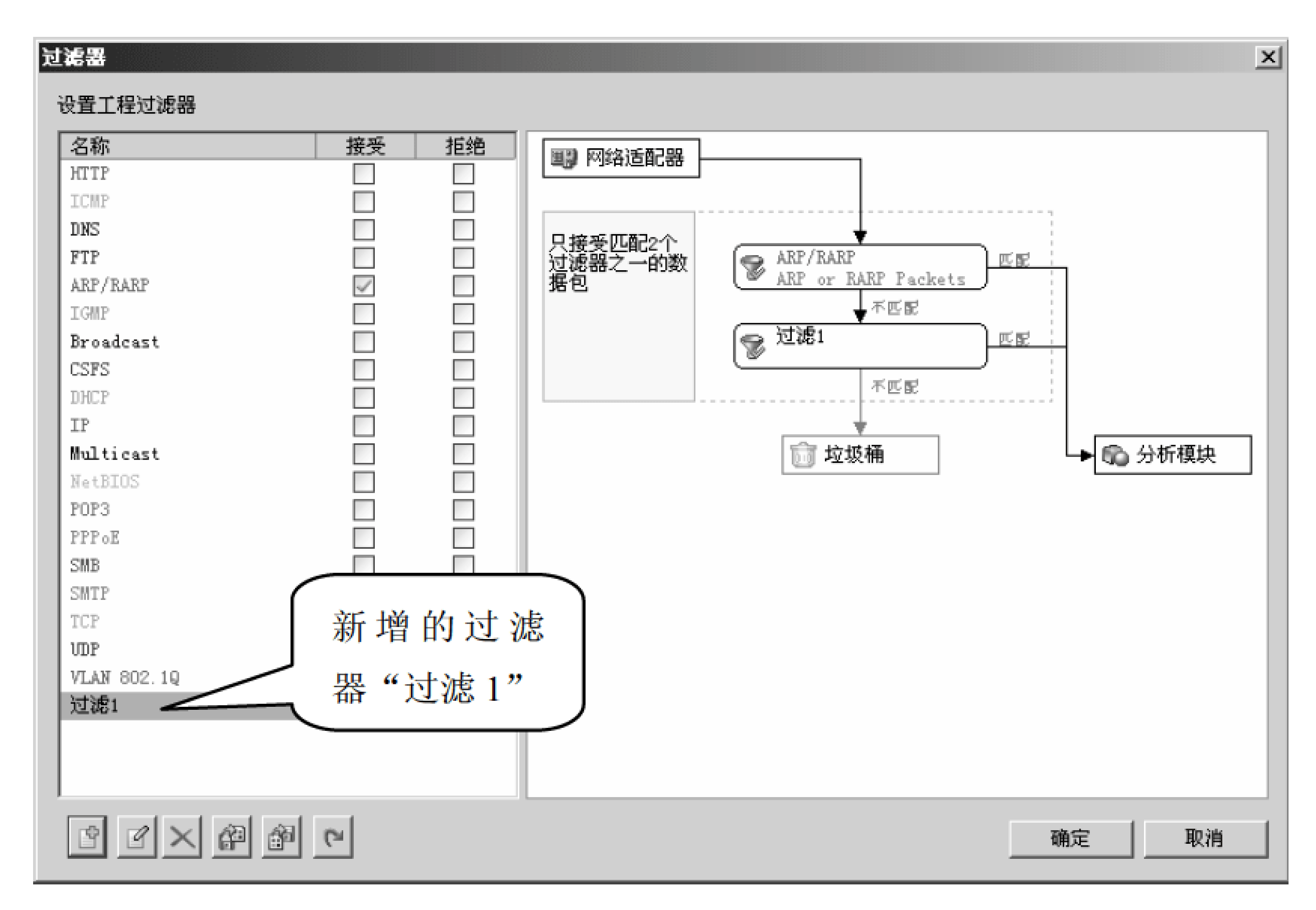


图 7-23

06 返回至科来网络分析系统的主程序界面，在右侧会看到捕捉过滤器为【已选择 2 个接受过滤器，只接受匹配的数据包】，表明设置捕捉过滤器成功，如图 7-24 所示。

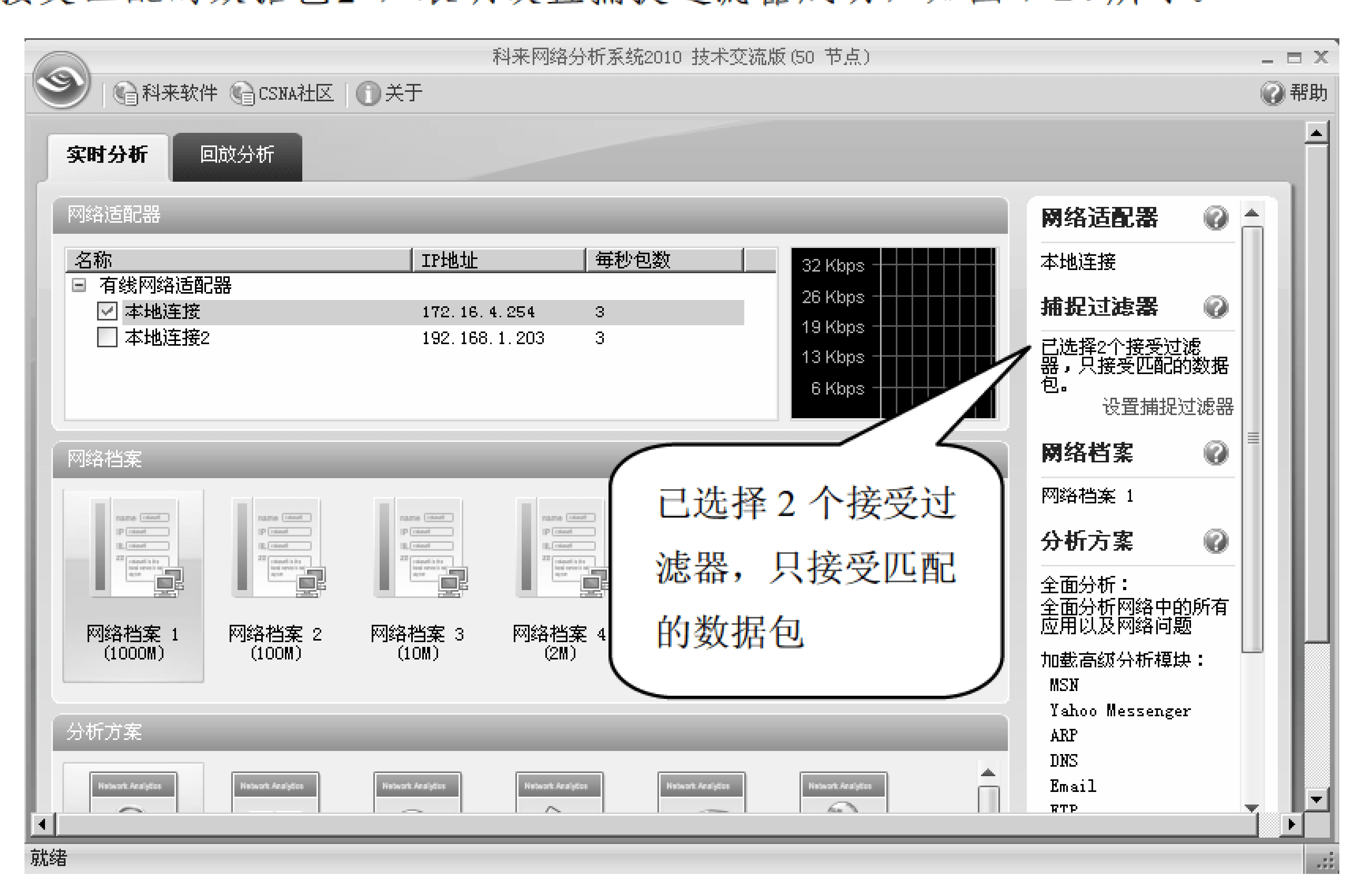


图 7-24

7.3.3 使用科来网络分析系统分析 ARP 异常

局域网通信依赖大量的 ARP 广播，但是很多病毒或者木马趁机利用 ARP 广播进行 ARP 攻击，严重影响局域网的畅通。

利用科来网络分析系统分析网络中 ARP 异常的具体操作步骤如下。

01 选择【开始】➢【所有程序】➢【科来网络分析系统 2010 技术交流版】➢【科来网络分

析系统 2010 技术交流版】菜单命令，打开科来网络分析系统，选择监听网卡【本地连接】复选框，单击右侧【设置捕捉过滤器】选项，如图 7-25 所示。



图 7-25

02 弹出【过滤器】窗口，选择【ARP/RARP】协议的【接收】复选框，表明要捕捉关于 ARP/RARP 协议相关的数据包，单击【确定】按钮，如图 7-26 所示。

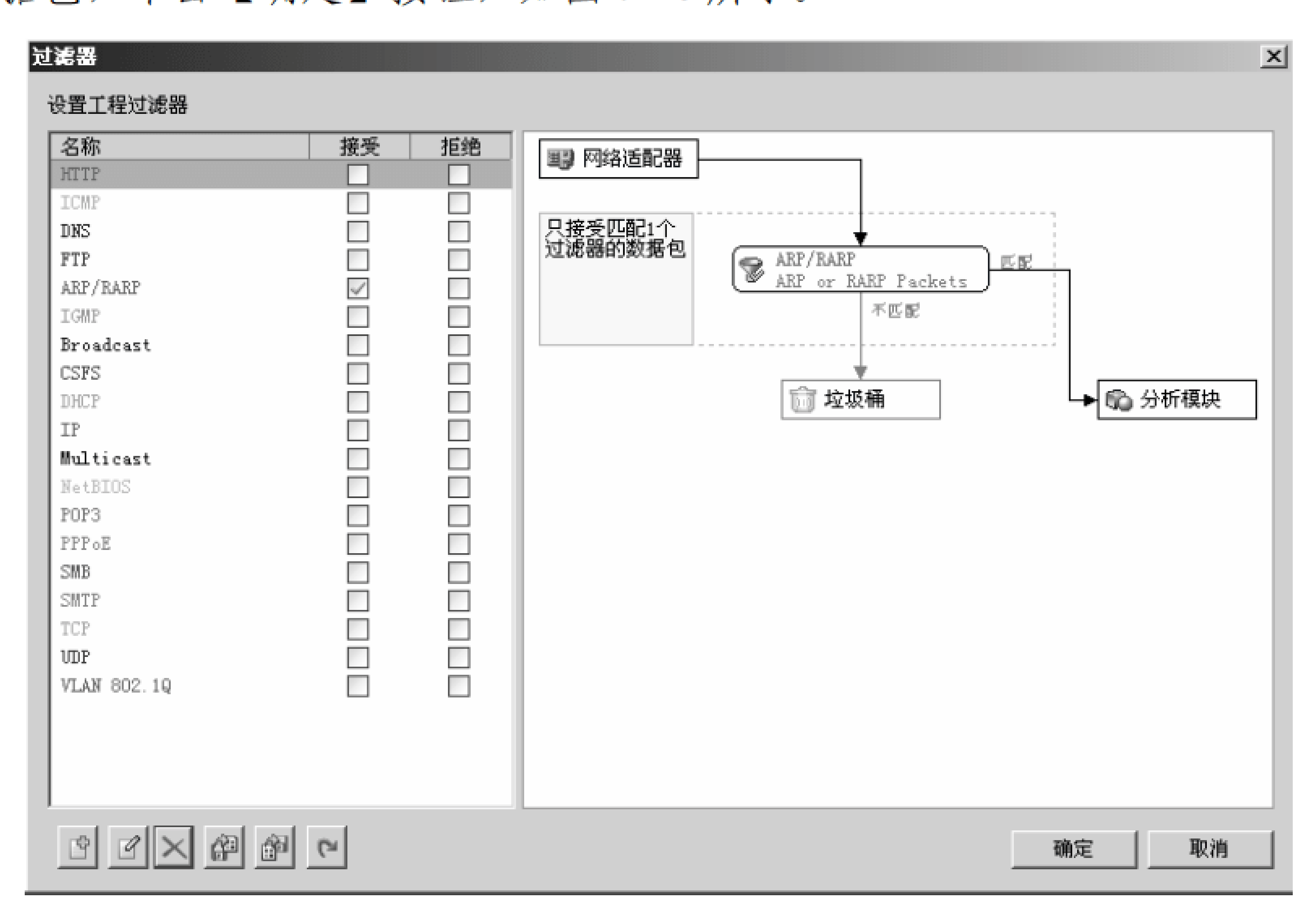


图 7-26

03 返回至科来网络分析系统程序主界面，单击右下角【开始】按钮，开始数据捕捉，如图 7-27 所示。



图 7-27

04 单击【停止】按钮，可以结束数据的捕捉，如图 7-28 所示。

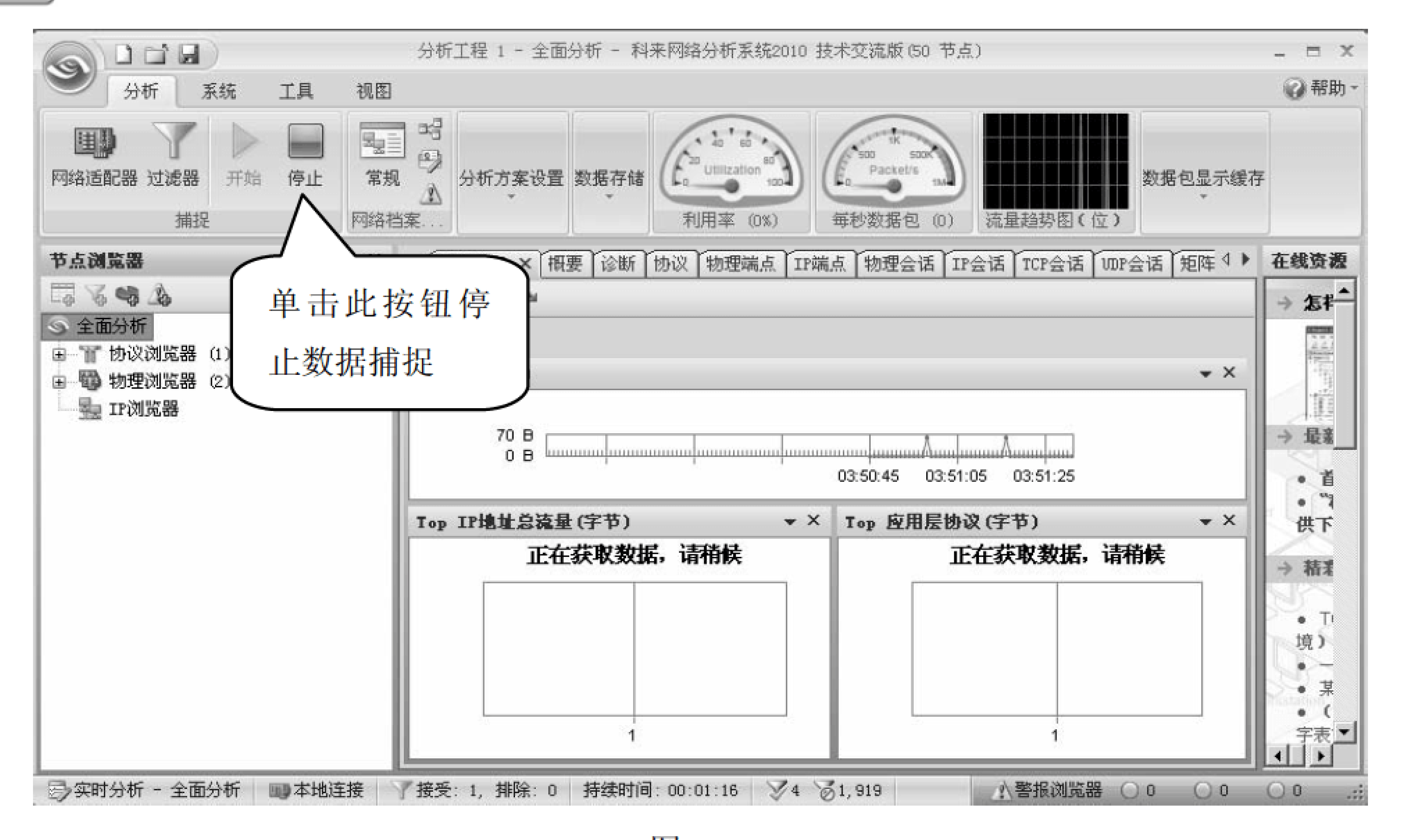


图 7-28

05 当数据捕获完成后，选择【协议】选项卡，在该窗口中可以看到网络中各个协议的使用比例情况，如果 ARP 协议使用比例过大，则可以怀疑网络是否中了 ARP 病毒或者某台主机正在进行 ARP 攻击，如图 7-29 所示。

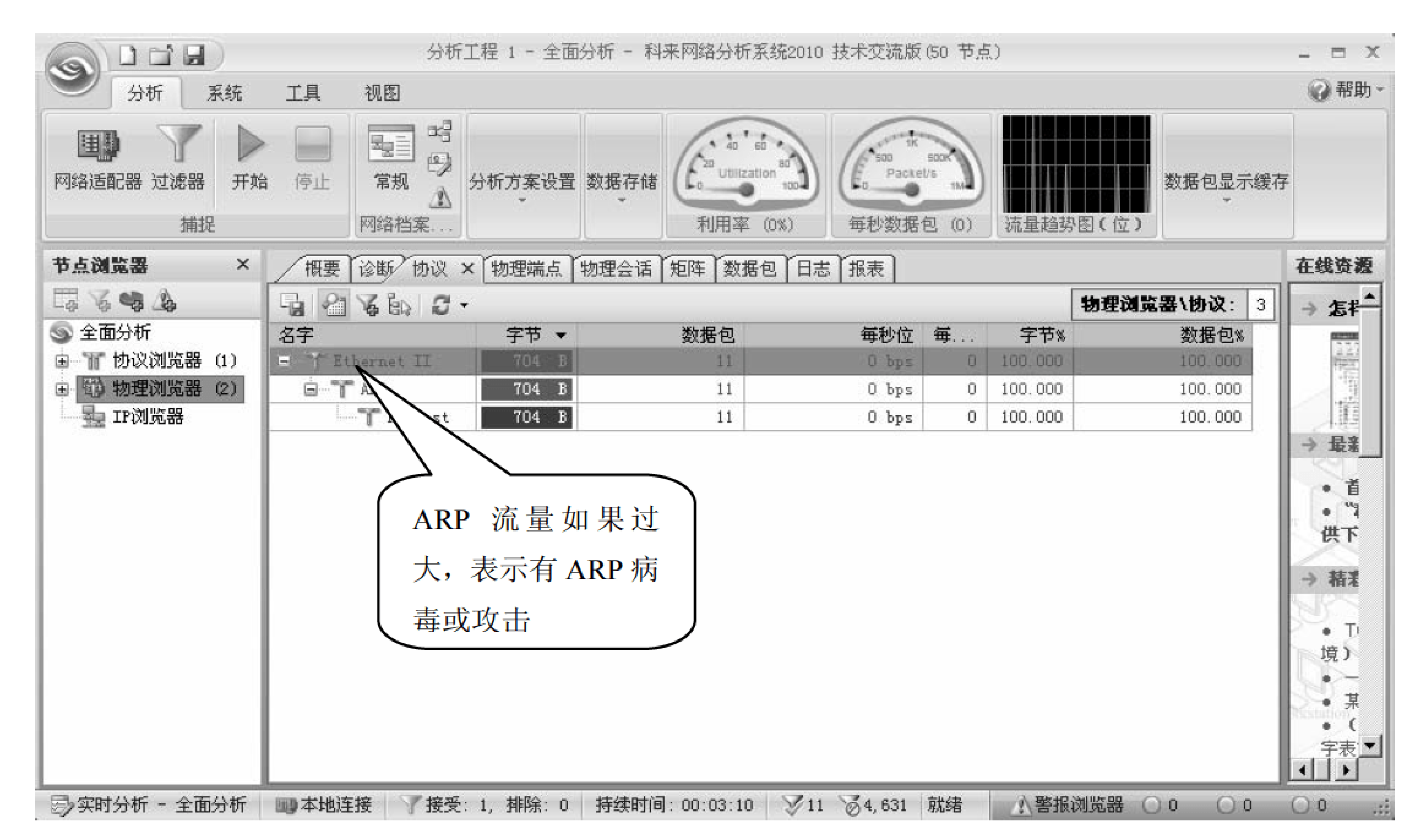


图 7-29

06 选择【数据包】选项卡，在打开的界面中可以查看科来网络分析系统捕捉到的数据包。从捕获结果中可以看出，在网络中哪些主机在进行 ARP 广播，如果发现某个主机一直和大量的主机进行 ARP 通信，则可以怀疑该主机正在进行 ARP 攻击，如图 7-30 所示。

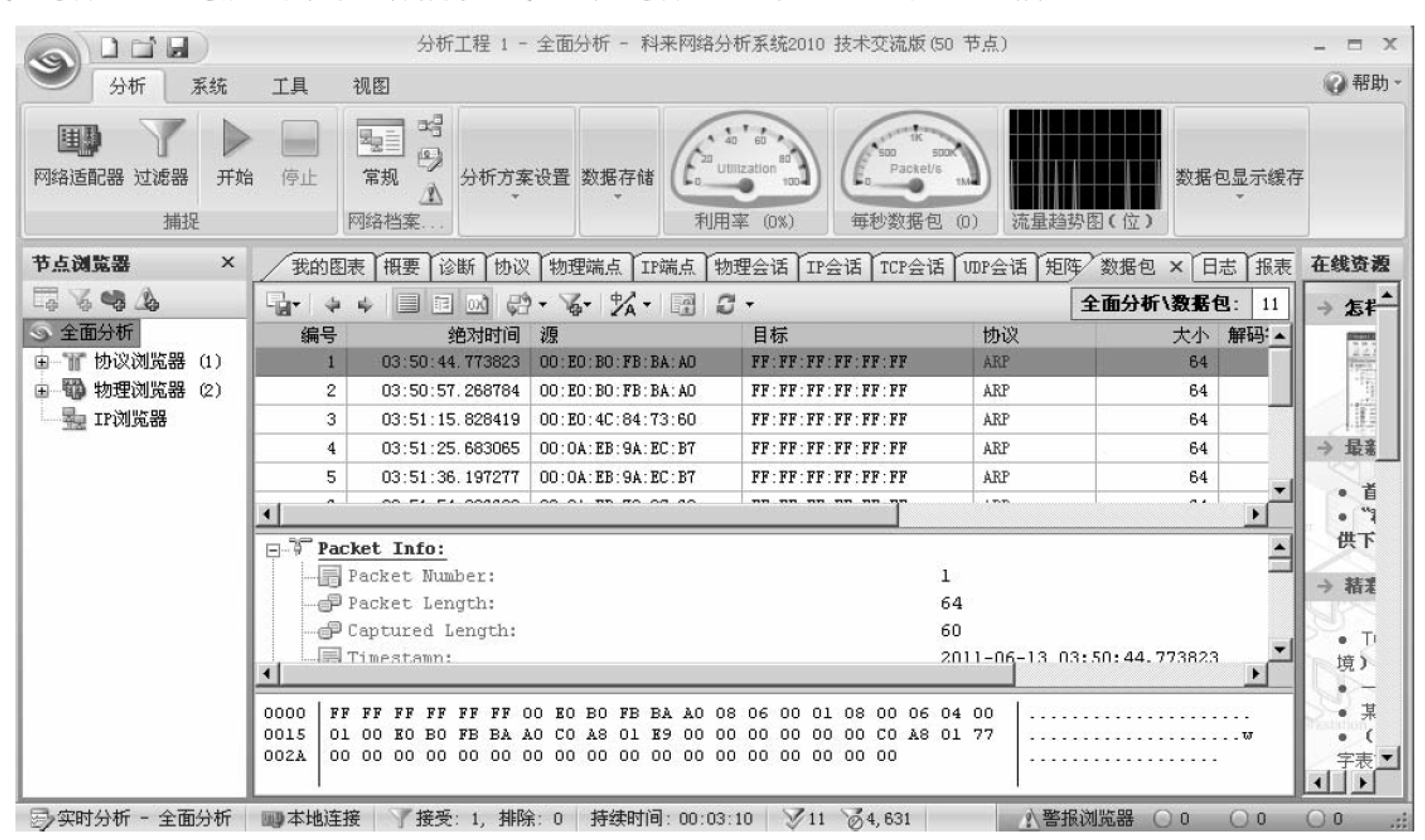


图 7-30

7.4 项目实施 2：使用 Sniffer Pro 进行网络流量监控分析

Sniffer Pro 的主要功能是捕获数据包然后进行分析，网络管理人员可以通过对捕获到的数据包进行分析，从而得到网络的运行情况。Sniffer Pro 提供的多种仪表盘可以帮助网络管理人员更加直观的获取网络中协议、计算机之间通信等运行信息，从而帮助网络管理人员及时解决网络故障。

7.4.1 安装 Sniffer Pro 网络嗅探工具

安装 Sniffer Pro 网络嗅探工具的具体操作步骤如下。

01 运行安装程序，弹出【Sniffer Portable】对话框，单击【Next】（下一步）按钮，如图 7-31 所示。



图 7-31

02 弹出【Setup】（安装）提示框口，Sniffer 安装正在继续，如图 7-32 所示。

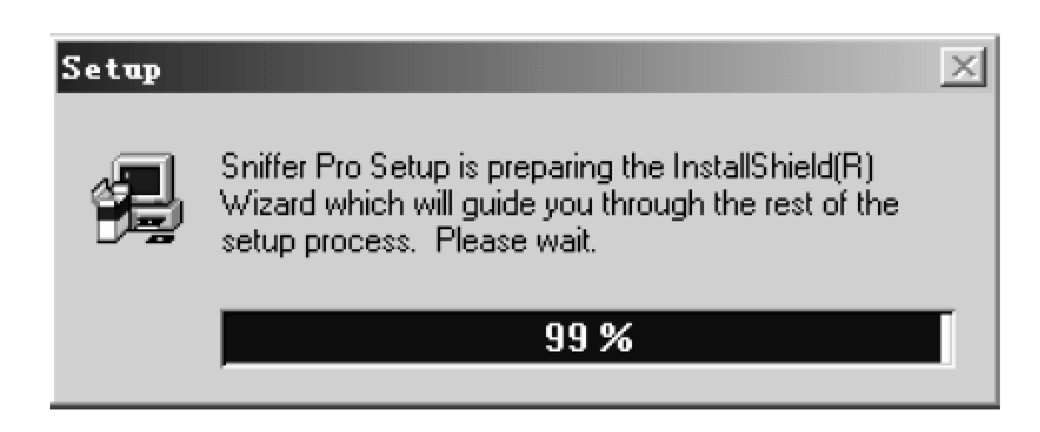


图 7-32

03 弹出【Welcome】（欢迎）对话框，单击【Next】（下一步）按钮，如图 7-33 所示。



图 7-33

04 弹出【Software License Agreement】（软件许可协议）对话框，单击【Yes】（是）按钮，表示同意 Sniffer Pro 的安装协议，如图 7-34 所示。

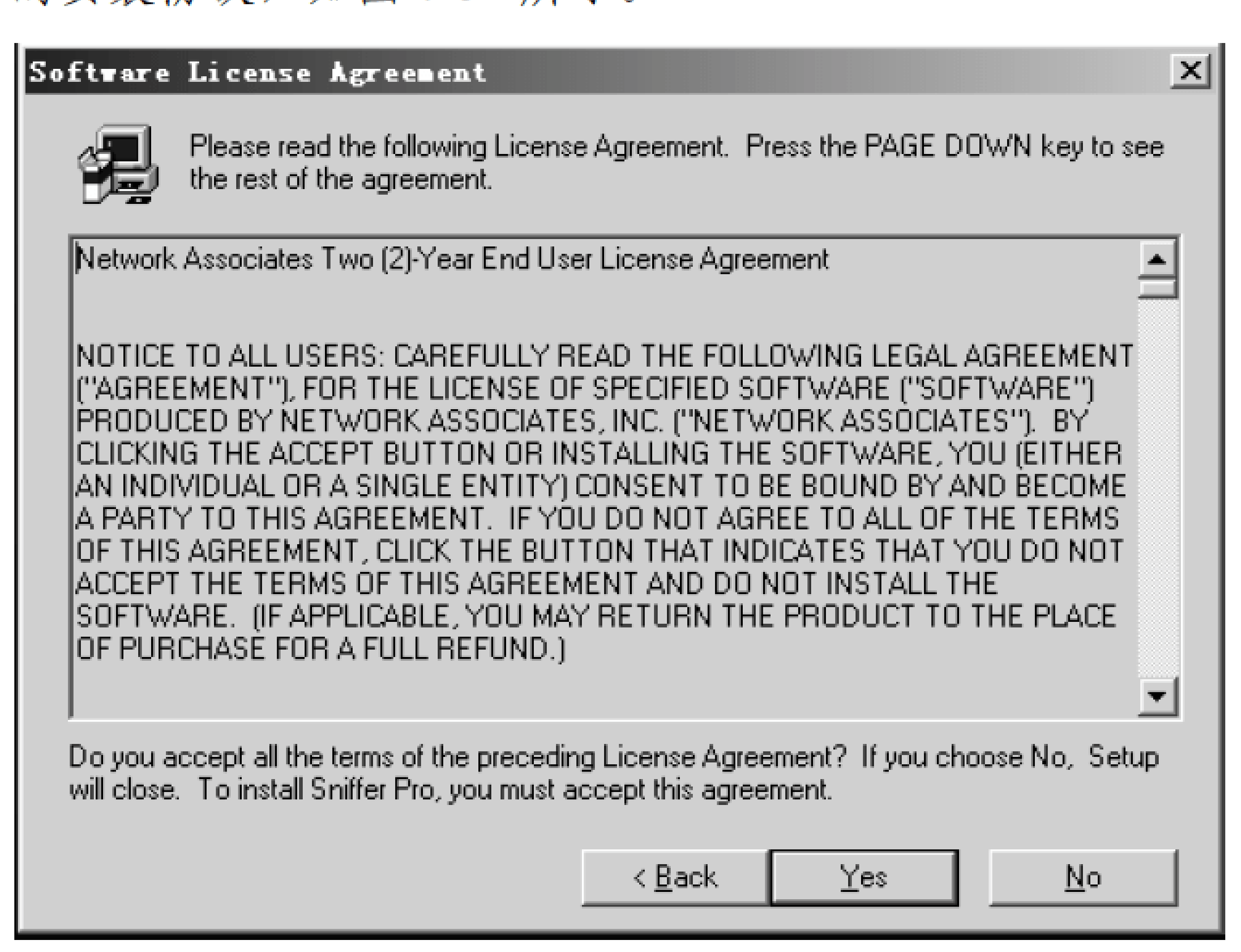


图 7-34

05 弹出【User Information】（用户信息）对话框，在【Name】（姓名）和【Company】（公司）文本框中分别输入用户的姓名和公司信息，本实例中输入姓名为“sushi”，公司为“yingda”，单击【Next】（下一步）按钮，如图 7-35 所示。

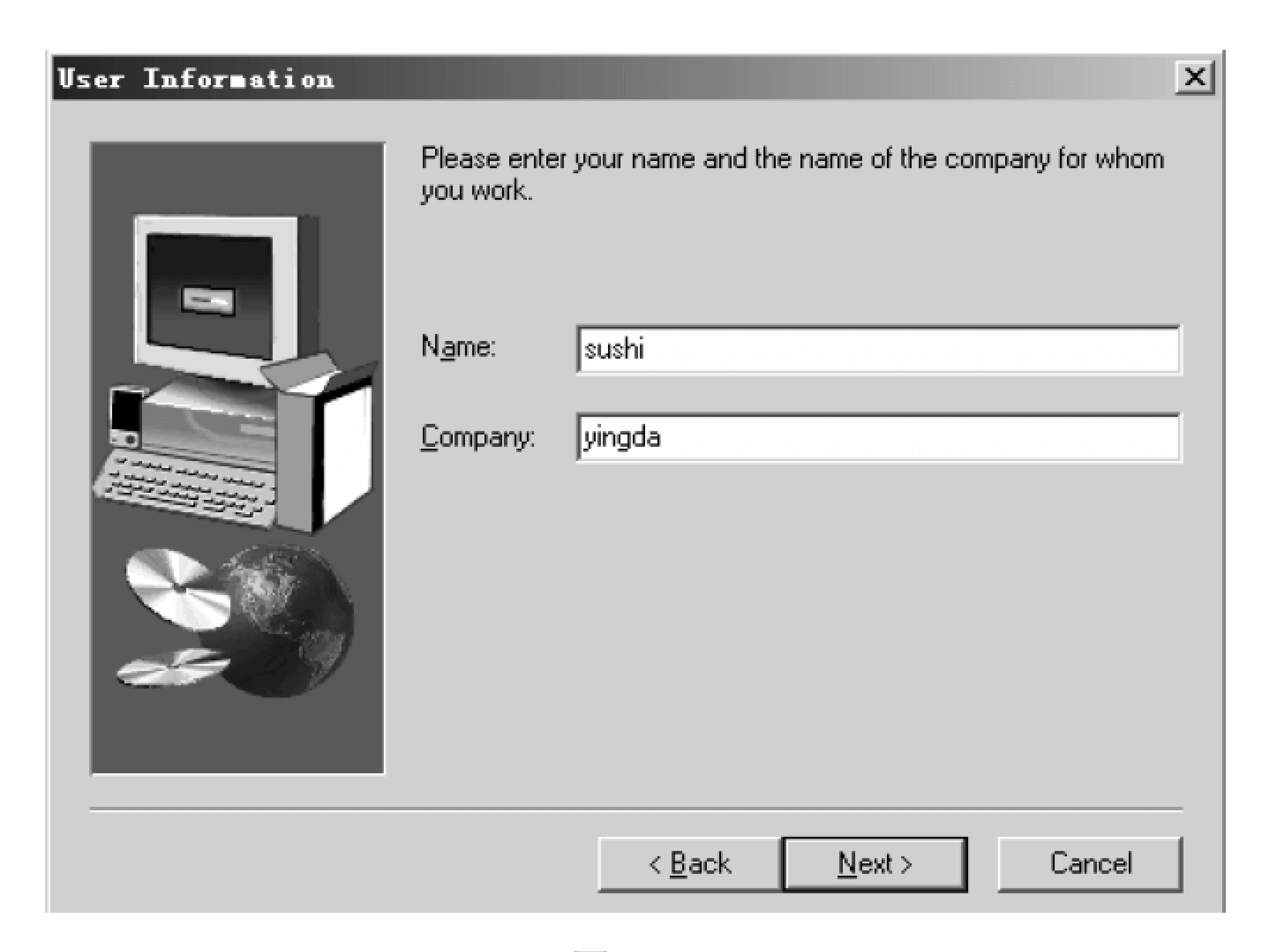


图 7-35

06 弹出【Choose Destination Location】（选择目标路径）对话框，单击【Browse】（浏览）按钮选择 Sniffer 的安装路径，默认安装路径“C:\Program Files\NAI\SnifferNT”，单击【Next】（下一步）按钮，如图 7-36 所示。



图 7-36

07 弹出【Sniffer Pro User Registration】（Sniffer Pro 用户注册）对话框，在【First Name】（第一个名字）、【Last Name】（最后一个名字）、【Business】（公司）、【Customer】（行业）和【E-mail】（邮箱）文本框中输入相关信息，注意如图 7-37 所示，每个文本框必须输入必要的信息，单击【下一步】按钮，如图 7-37 所示。

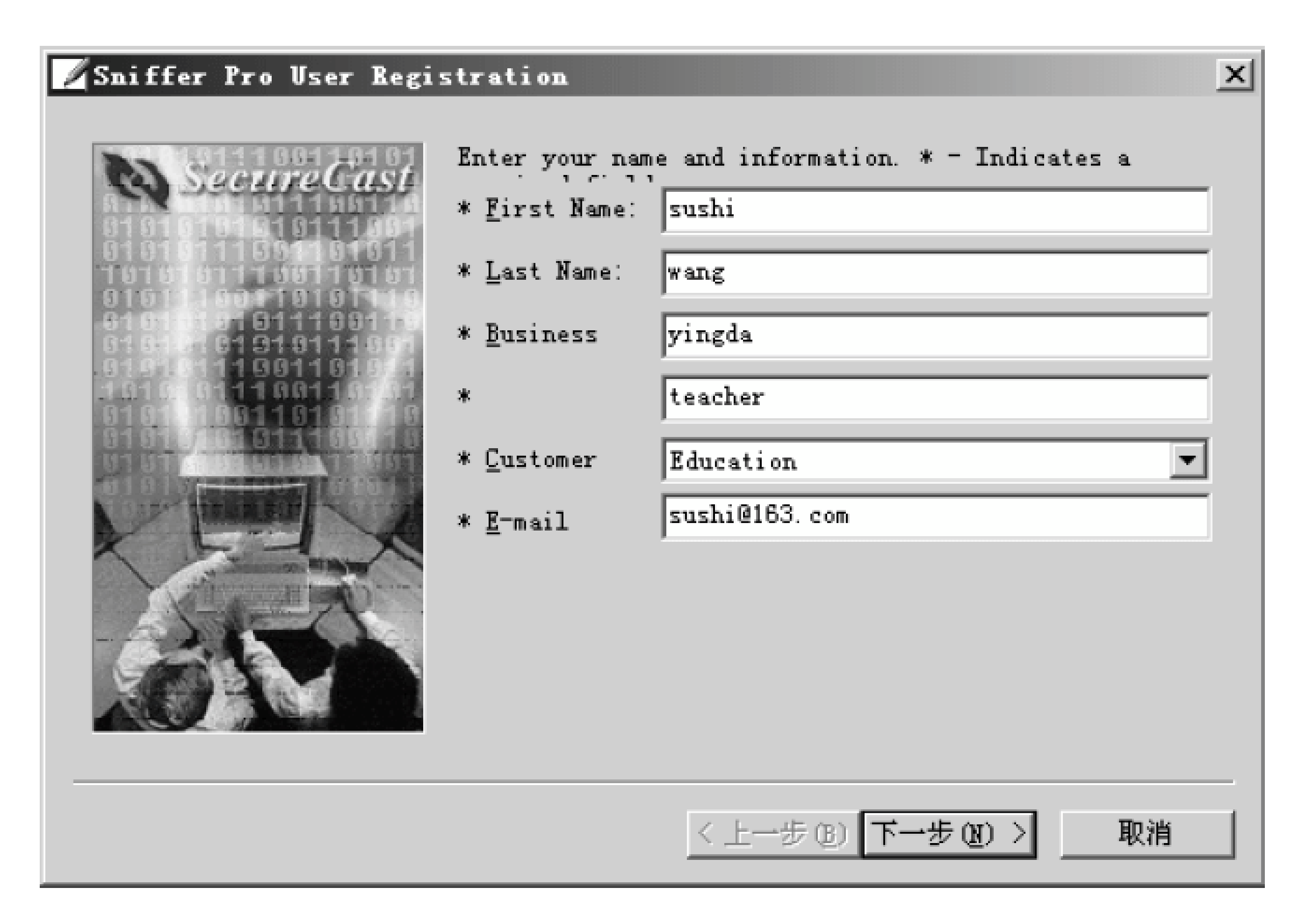


图 7-37

08 弹出【Sniffer Pro User Registration】（Sniffer Pro 用户注册）对话框，在【Address】（地址）、【City】（城市）、【Country】（国家）、【Postal】（邮编）、【Phone】（电话）和【Fax Number】（传真号码）文本框中输入相关信息，单击【下一步】按钮，如图 7-38 所示。



图 7-38

09 弹出【Sniffer Pro User Registration】（Sniffer Pro 用户注册）对话框，在【Please let us know where you heard about this product】（请让我们知道你是在哪里听到关于这个产品的信息）文本框中选择用户是通过什么渠道获得关于 Sniffer 的信息，在【Do you wish to receive announcements about this product】（你是否希望接受关于这个产品的广告）文本框中选择否愿意接收和 Sniffer 有关的广告，在【May we share your name with other companies that use NAI products】（我们是否可以和其他公司分享你使用这个产品的信息）文本框选择否愿意让其他的公司知道你们正在使用 Sniffer，在【Sniffer Serial Number】（Sniffer 序列号）文本框中输入 Sniffer 的产品密钥，单击【下一步】按钮，如图 7-39 所示。



图 7-39

10 弹出【Sniffer Pro User Registration】（Sniffer Pro 用户注册）对话框，选择用户如何接入互联网的。有三个选项分别为：【Direct Connection to the Internet】（直接接入互联网）、【Connection to the Internet through a Proxy】（通过代理接入互联网）和【Not connected to network or Dial-up Print & fax option】（没有接入互联网或者通过电话和传真接入互联网）。这里选择没有接入互联网，单击【下一步】按钮，如图 7-40 所示。

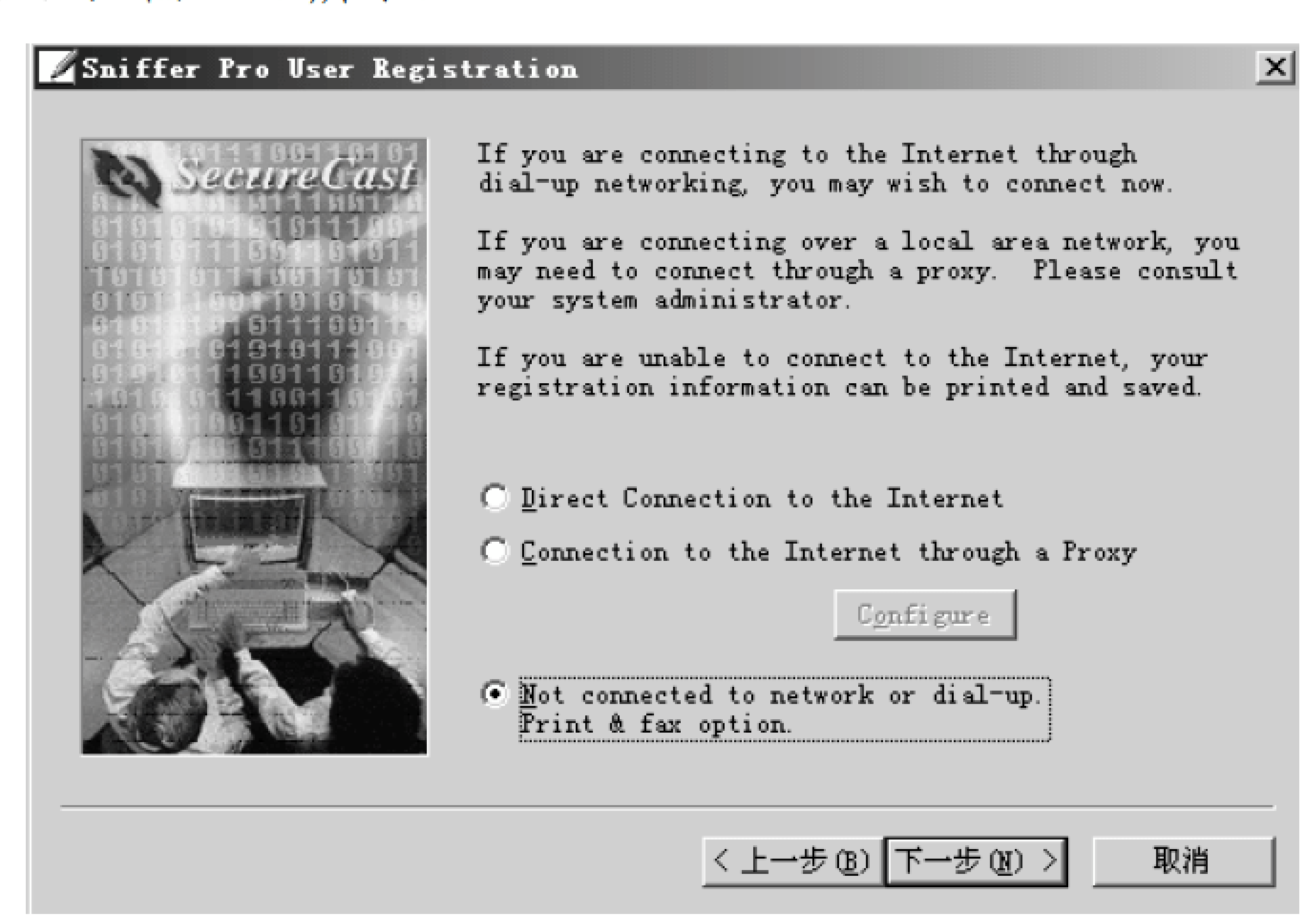


图 7-40

11 弹出【Sniffer Pro User Registration】（Sniffer Pro 用户注册）对话框，单击【完成】按钮，完成 Sniffer 的注册，如图 7-41 所示。



图 7-41

12 弹出【Setup Complete】（安装完成）对话框，单击【Finish】（完成）按钮，如图 7-42 所示。

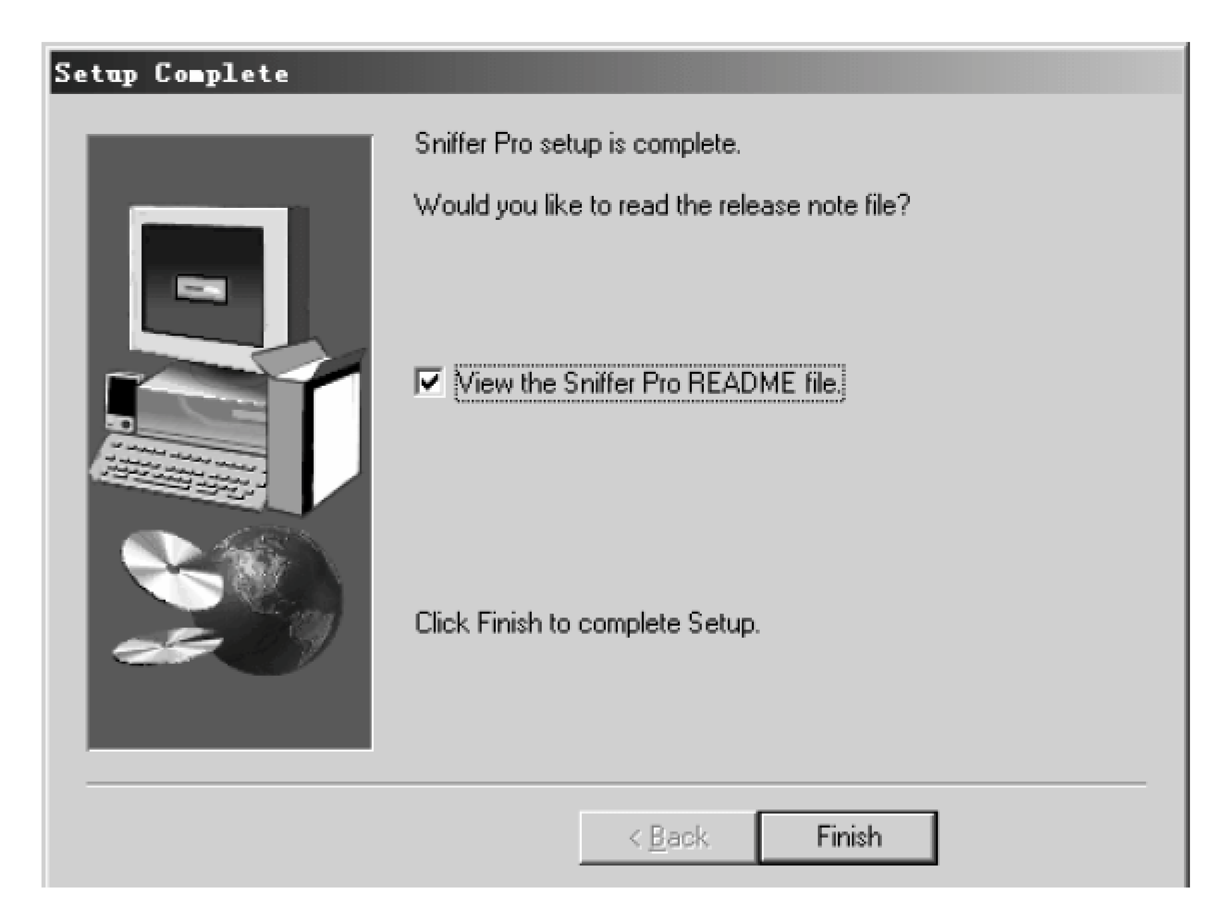


图 7-42

13 弹出【Setup Complete】(安装完成)对话框，选择【Yes，I want to restart my computer now】（是的，我想现在重新启动我的计算机）选项，单击【Finish】（完成）按钮，如图 7-43 所示。



图 7-43

14 计算机重启过之后，Sniffer Pro 安装完成。但是要想完整的显示 Sniffer Pro 操作界面，还必须安装 JDK 软件包，双击 JDK 安装文件，弹出【Java(TM) SE Development Kit 6 update 10 – 许可证】（JDK6.10 安装许可证）对话框，单击【接受】按钮，如图 7-44 所示。

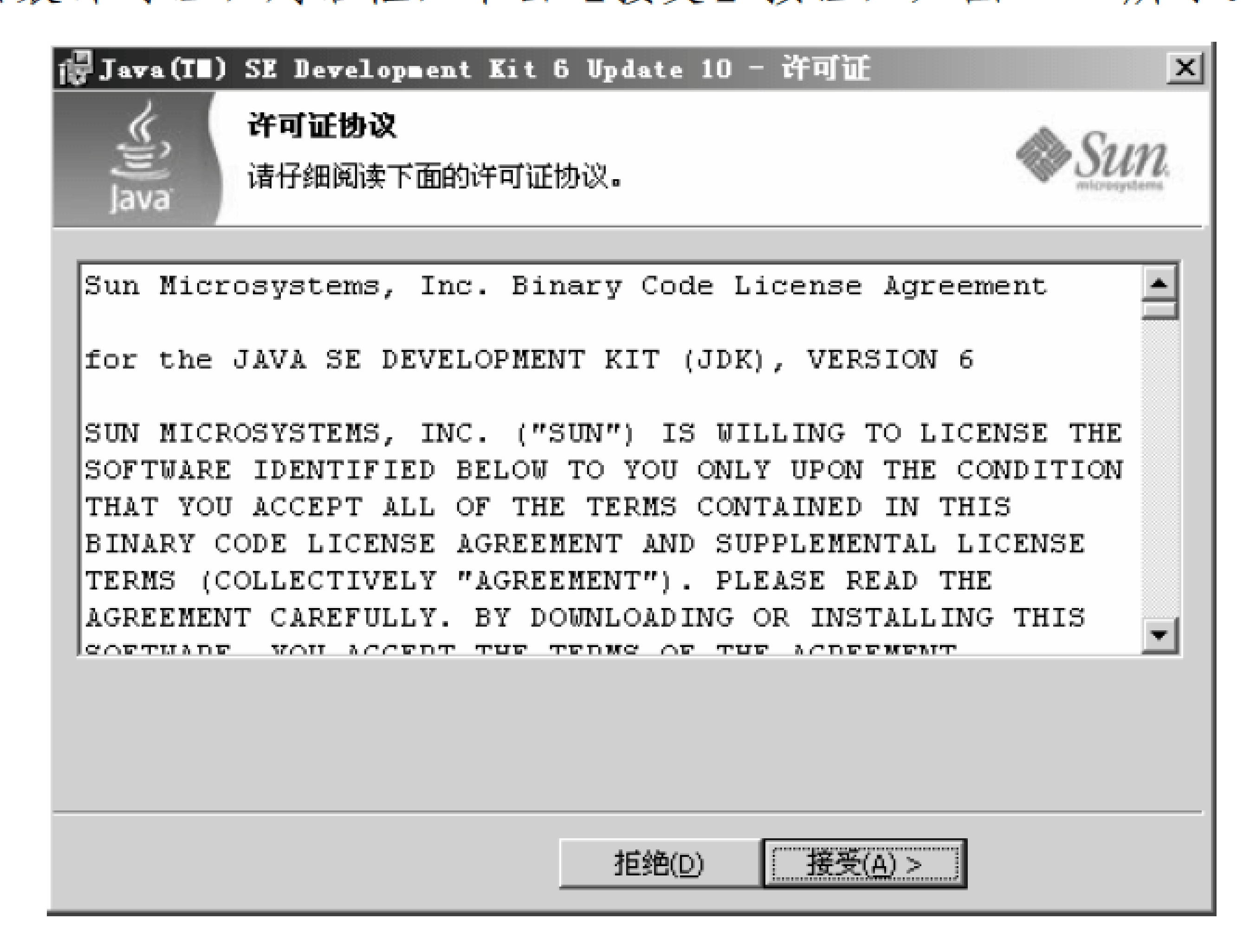


图 7-44

15 弹出【自定义安装】对话框，单击【更改】按钮自定义 JDK 的安装路径，单击【下一步】按钮，如图 7-45 所示。

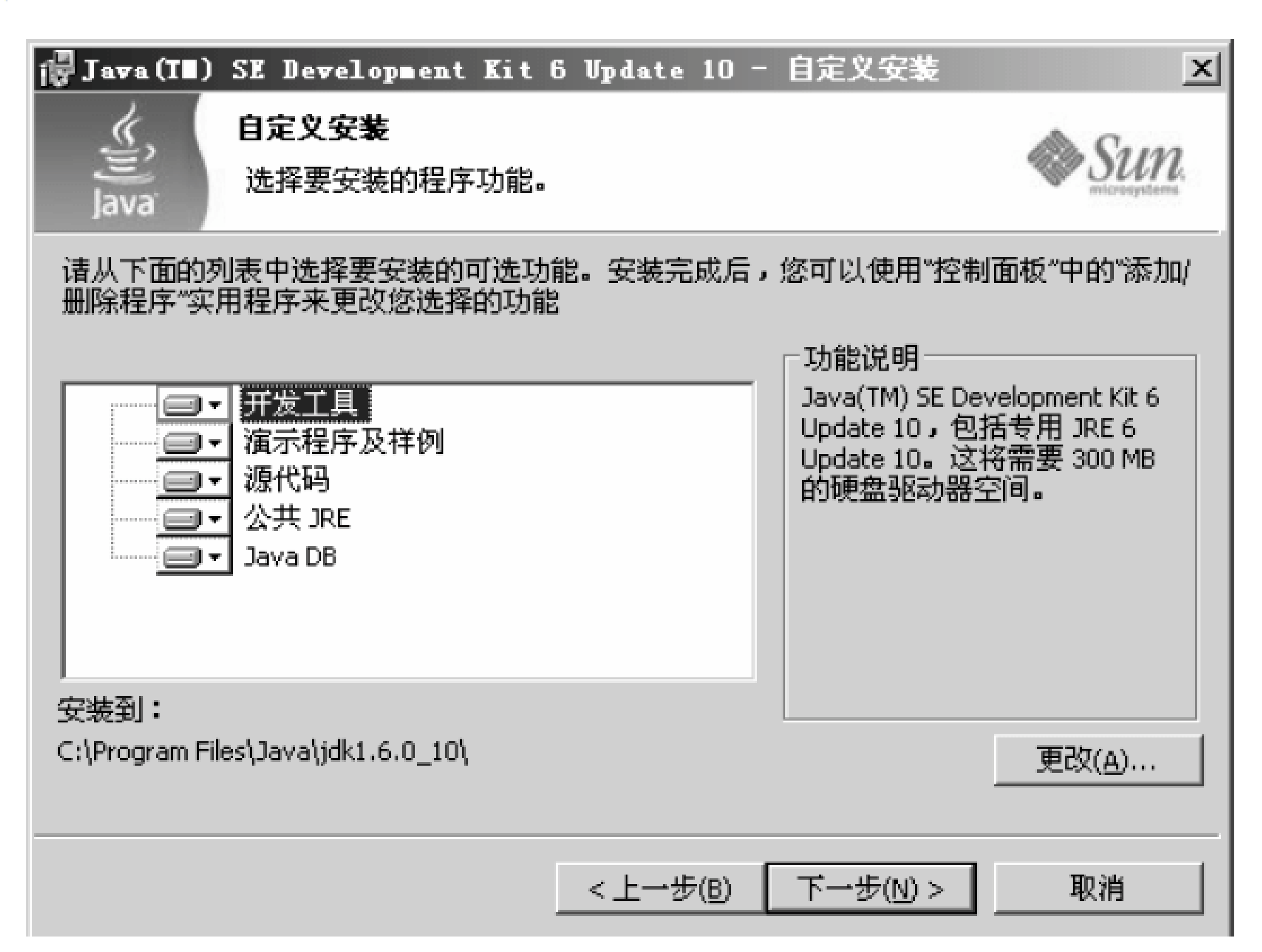


图 7-45

16 JDK 安装程序正在继续安装，显示安装进度，如图 7-46 所示。



图 7-46

17 弹出【目标文件夹】对话框，单击【更改】按钮自定义 Java 安装路径，单击【下一步】按钮，如图 7-47 所示。



图 7-47

18 JDK 安装程序正在继续安装，并显示安装进度，如图 7-48 所示。



图 7-48

19 JDK 安装结束，单击【完成】按钮，完成 JDK 的安装，如图 7-49 所示。



图 7-49

7.4.2 设置 Sniffer Pro 监控网络适配器

如果安装 Sniffer 的服务器有两块以上的网卡，就需要设置 Sniffer Pro 的监听网卡。由于所有的局域网数据包都通过代理服务器的内网网卡连接互联网，所以如果想要监听内网与外网的所有通信，就需要 Sniffer Pro 监控代理服务器的内网网卡。

具体的操作步骤如下。

01 选择【开始】➢【所有程序】➢【Sniffer Pro】➢【Sniffer】菜单命令，打开 Sniffer Pro 软件，如图 7-50 所示。



图 7-50

02 弹出【Settings】（设置）对话框，选择代理服务器的内网网卡也就是 Sniffer Pro 要监控的网卡，单击【确定】按钮，如图 7-51 所示。

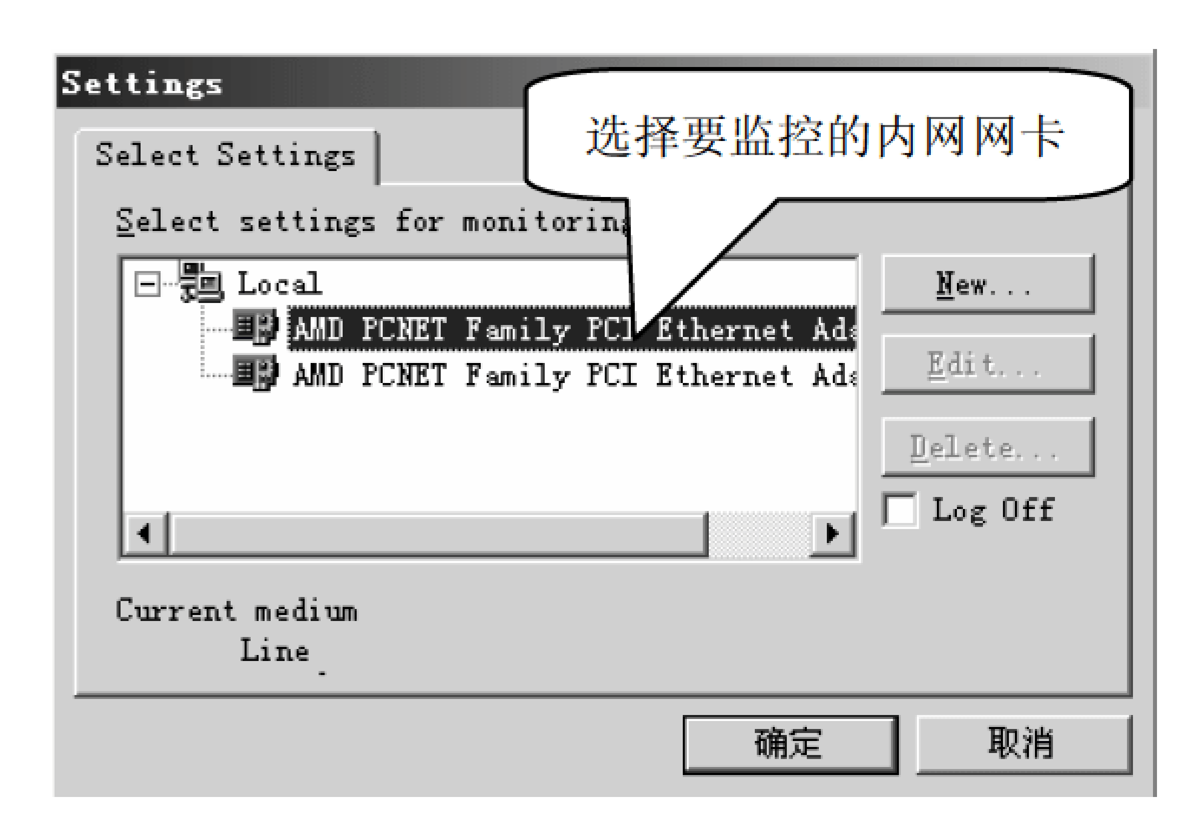


图 7-51

03 弹出 Sniffer Pro 程序的主界面，主界面由工具栏、仪表盘、流量统计 3 部分构成，如图 7-52 所示。

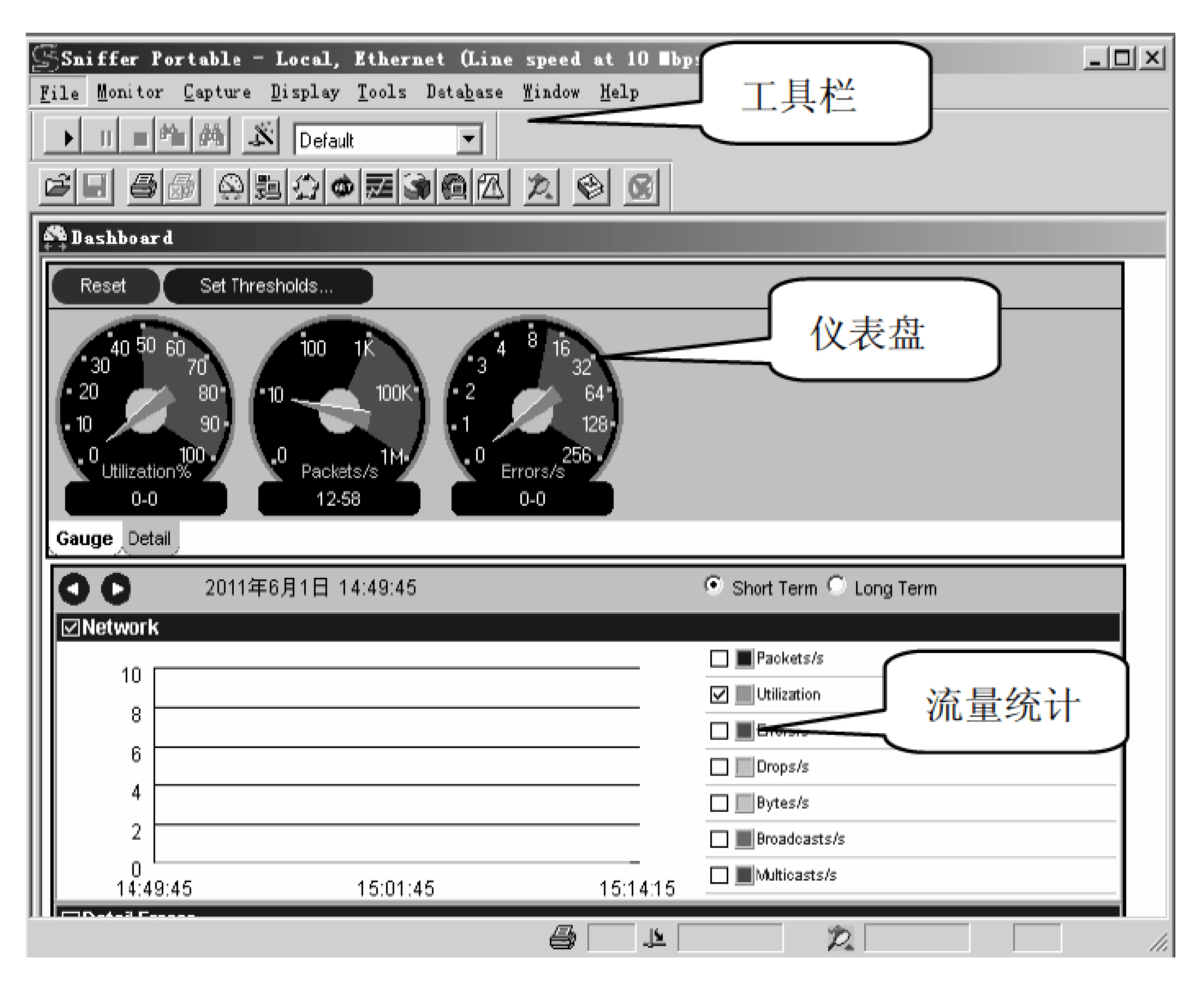


图 7-52

7.4.3　Sniffer 的监控功能

Sniffer 的主要功能是监控网络中数据包的传输。Sniffer 主要有 7 大监控功能，包括 Dashboard（仪表）、Host Table（主机列表）、Matrix（矩阵）、ART（应用响应时间）、Protocol Distribution（协议分类）、History Sample（历史采样）和 Global Statistics（球状统计）。合理使用这些功能可以帮助网络管理员实时的查看网络中传输的数据，便于网络管理员及时发现故障并解决。

1. Dashboard（仪表）

Sniffer Pro 使用各种仪表盘将捕捉到的数据包以人性化的方式显示，熟练使用 Sniffer Pro 的各种仪表盘有助于快速的分析数据包并解决问题。

Sniffer Pro 仪表盘使用图形化界面，可以直观地检测到网络的利用情况。具体的操作步骤如下。

01 在 Sniffer Pro 的程序主界面单击选择【Monitor】（监控）➢【Dashboard】（仪表）菜单命令，可以打开 Sniffer Pro 仪表盘。Sniffer Pro 的仪表盘有【Utilization%】（利用率百分比）、【Packets/s】（每秒传输的数据包）和【Error/s】（每秒产生的错误）三个表盘，如图 7-53 所示。

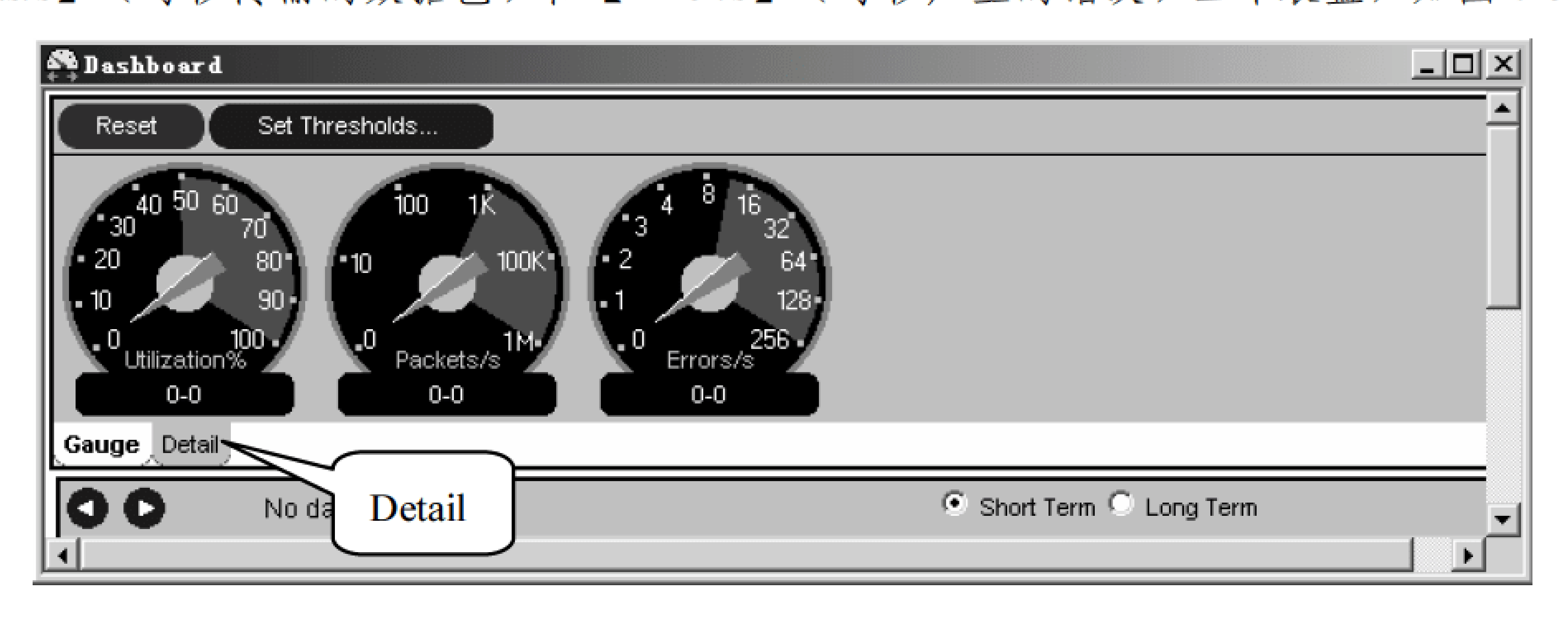


图 7-53



提 示

Sniffer Pro 的三个仪表盘下面都有两个数字，前面一个数字是当前值，后面一个数字是最大值。

三个仪表盘的含义如下。

- 【Utilization%】(利用率百分比)：表示网络带宽利用率，也就是现在网络流量所占带宽占总带宽的百分比。利用率百分比应该根据不同的网路情况来进行区分，不同的网络或者不同的网络拓扑，网络带宽利用率不一样。比如以太网网络的网络带宽如果能超过 40%就算很高了，但是全双工以太网中网络带宽需要达到 80%才算高。
- 【Packets/s】(每秒传输的数据包)：每秒钟传输的数据包可以帮助管理员更深入地了解每秒钟网络中传输帧的大小。通过每秒钟传输的数据包可以分析出当前网络传输速度，当网络利用率较小，但数据传输速度比较快时，就表明网络中传输的数据包较小。
- 【Error/s】(每秒产生的错误)：每秒产生的错误数据包数。很多网络管理员一听到错误数据包数量，就认为如果每秒钟产生的错误过多就是网络出现了问题，其实并非每个错误数据包都会带来网络问题。比如在以太网中产生的数据包冲突也是错误数据包造成的，但这种数据包只要不是过多就不会带来问题。

02 如果想要查看数据包的详细信息，单击在【Utilization%】（利用率百分比）仪表盘下面的【Detail】（详细信息）选项，打开详细信息界面，在其中查看相关的详细信息。单击仪表盘上的【Set Thresholds】（设置阈值）按钮，如图 7-54 所示。

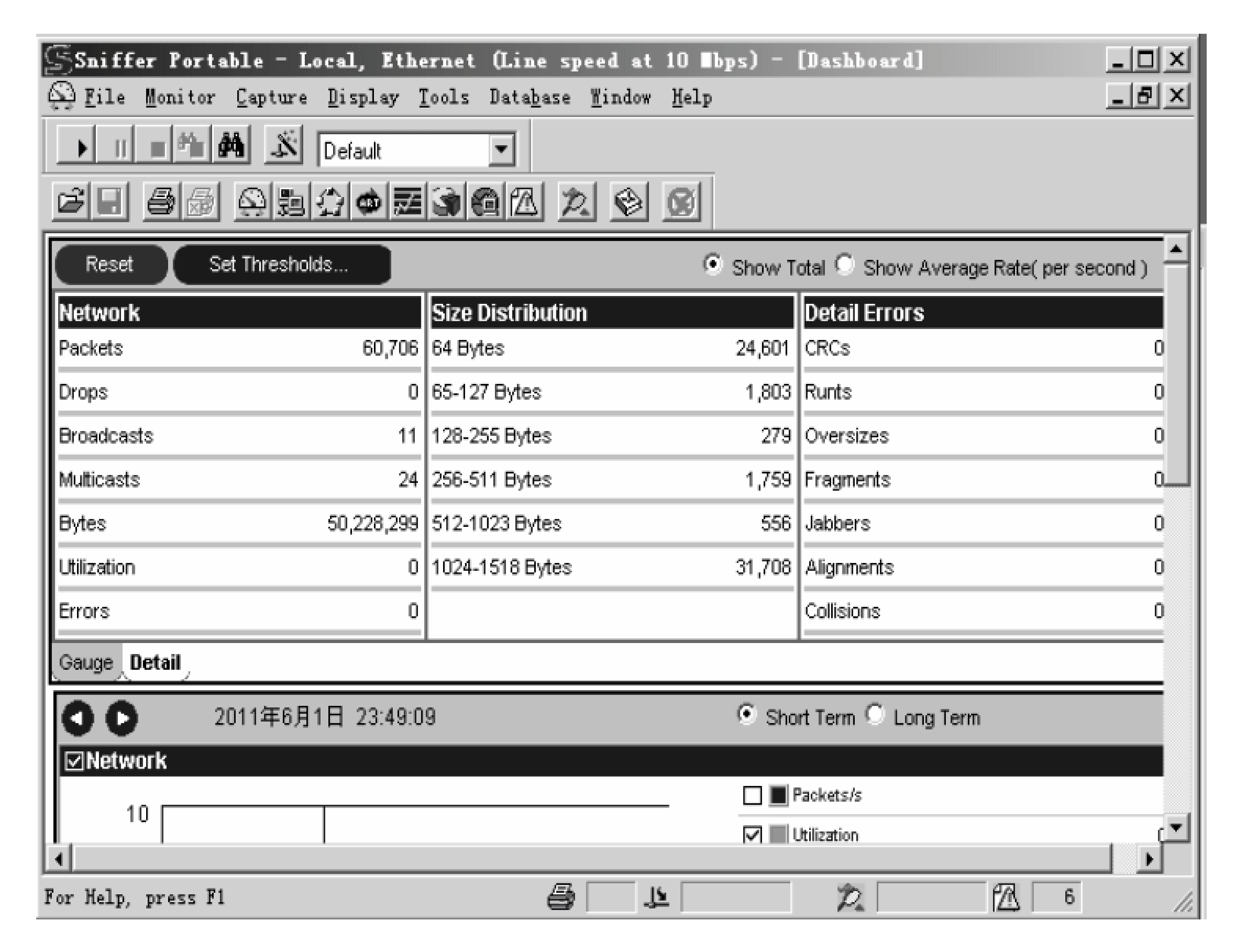


图 7-54

03 弹出【Dashboard Properties】（仪表盘内容）对话框，可以设定仪表盘的阈值，当网络中的流量达到一定数值，既阈值时，Sniffer Pro 用红色进行报警，如图 7-55 所示。

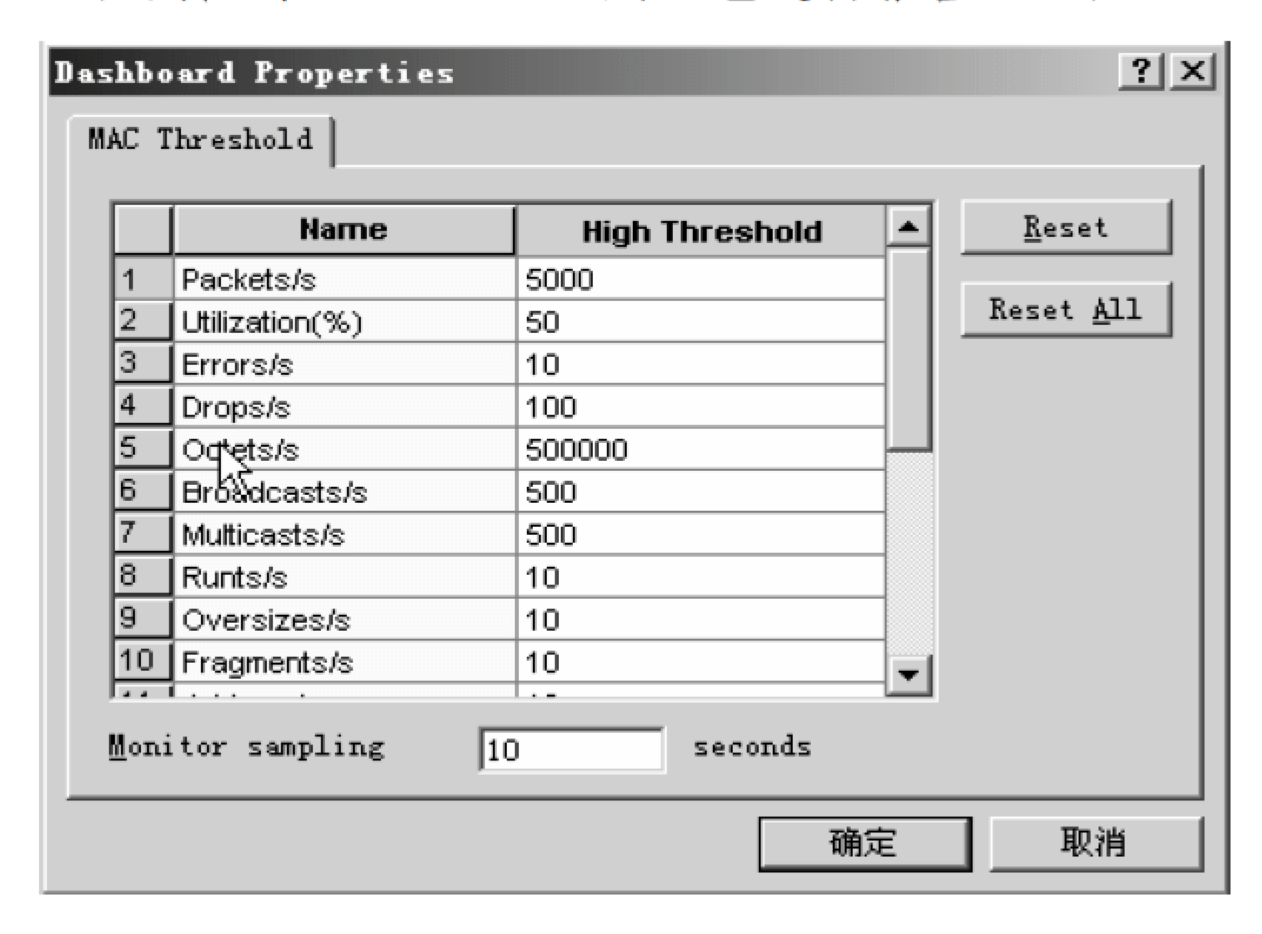


图 7-55

2. Host Table（主机列表）

Host Table（主机列表）以列表的形式显示了当前网络中计算机的通信信息，包含发送数据包、接收数据包和错误数据包等信息。如果一个主机在一定的时间内发送或者接收了大量的数据包，就可以怀疑该计算机正在使用 BT、P2P 等下载软件。

以主机列表形式查看计算机通信信息的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面单击菜单【Monitor】（监控）➢【Host Table】（主机列表）选项，打开【Host Table】（主机列表）对话框。列出了当前捕捉到的网络主机通信信息，如图 7-56 所示。

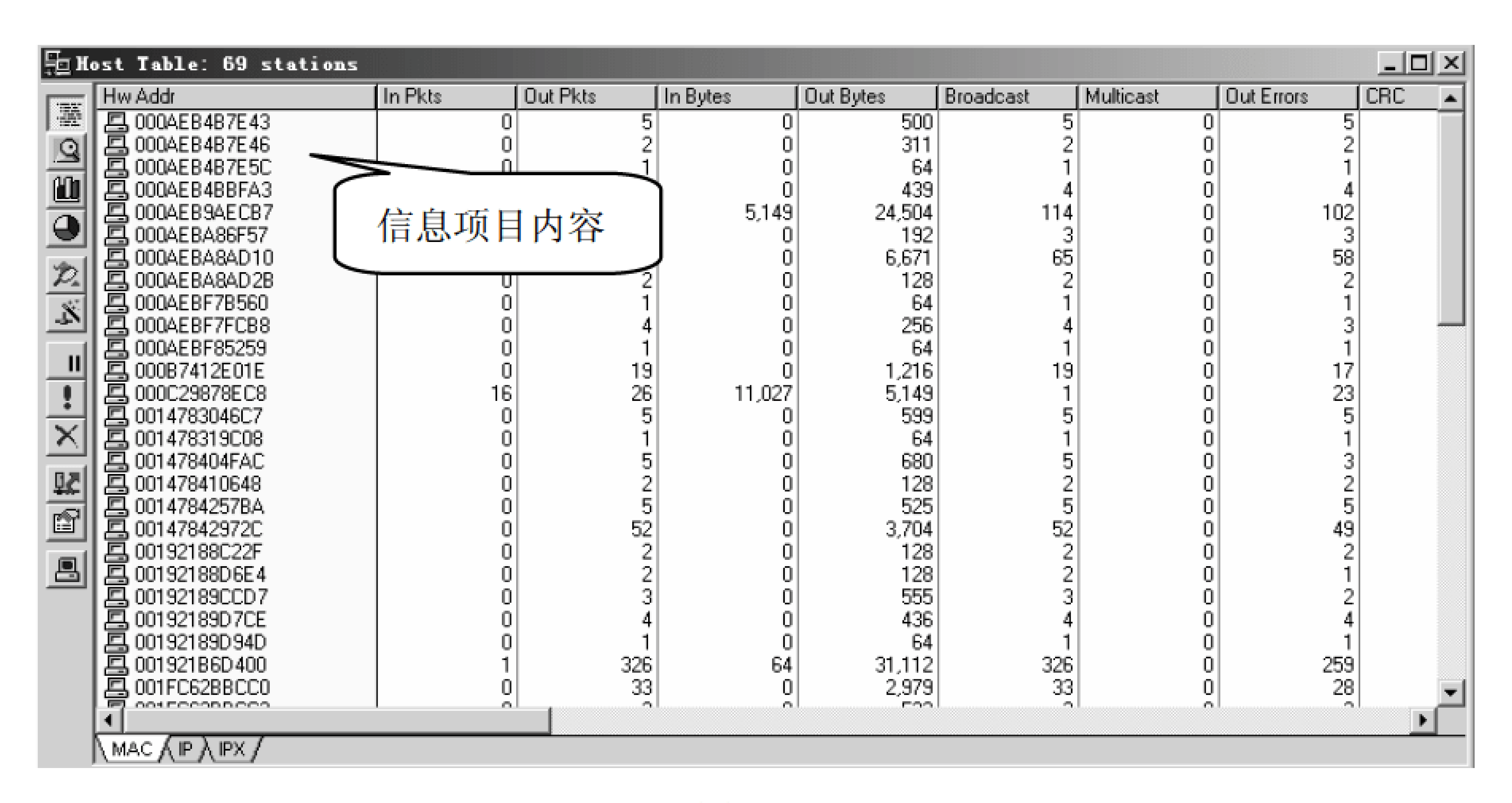


图 7-56

显示的信息项目内容解释如下。

- 【Hw Addr】(硬件地址): 默认情况下，主机列表以 MAC 地址的形式表示通信主机。
- 【In Pkts】(传入数据包): 此主机接收的数据包。
- 【Out Pkts】(传出数据包): 此主机发送的数据包。
- 【In Byts】(传入字节数): 此主机接收的字节数。
- 【Out Bytes】(传出字节数): 此主机发送的字节数。
- 【Broadcast】(广播数据包): 此主机广播的数据包。
- 【Out Errors】(传输的错误数据包): 此主机传出的错误数据包。

02 单击【Host Table】(主机列表)对话框左下方的【IP】选项，则 Sniffer Pro 将以 IP 地址的形式表示捕捉到的网络主机，如图 7-57 所示。

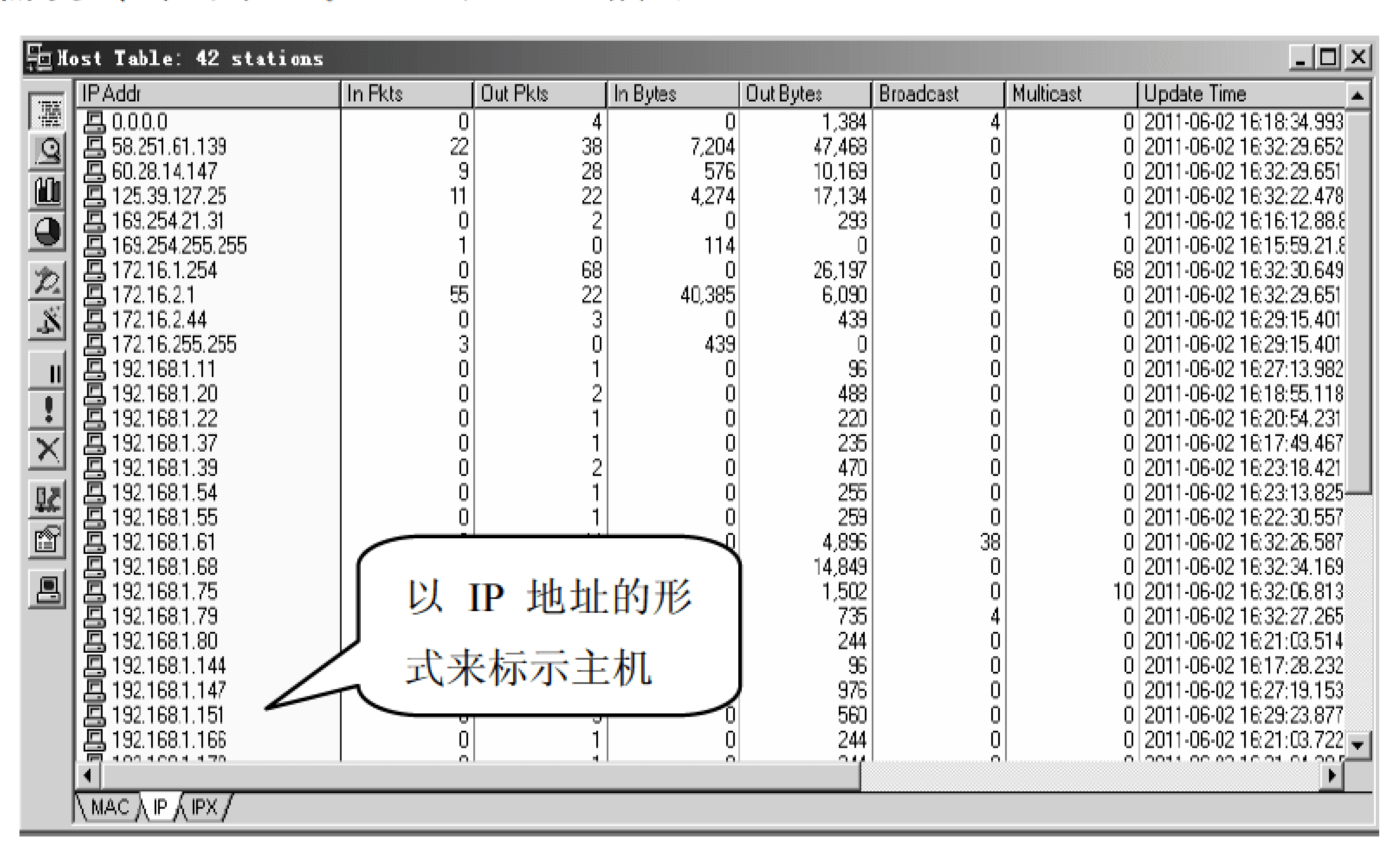


图 7-57

3. Matrix（矩阵）

Matrix（矩阵）以矩阵的形式来显示当前的网络通信信息，通过矩阵可以清晰看到网络中的主

机正在与哪些主机进行通信，当某个主机不停地和大量的主机同时进行通信时，就可以怀疑该主机是否中了蠕虫病毒或者正在使用 BT、P2P 等下载软件。

以矩阵方式查看网络通信信息的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面单击菜单【Monitor】（监控）➢【Matrix】（矩阵）选项，打开【Matrix】（矩阵）对话框。列出了当前捕捉到的网络主机通信信息，默认情况下在矩阵中以 MAC 地址的形式来表示网络中的主机，如图 7-58 所示。

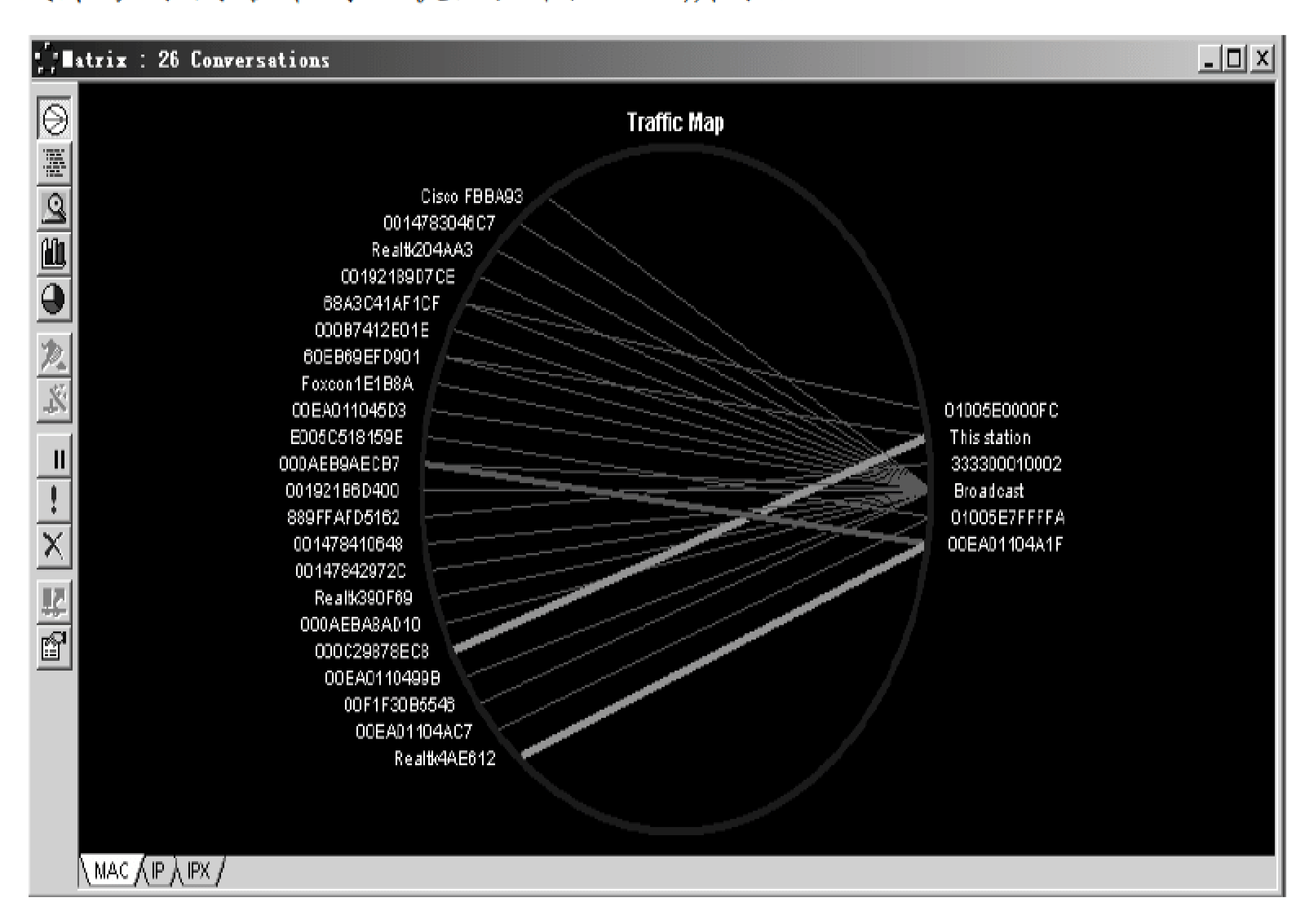


图 7-58

上图中线条的颜色表示相应的通信状态如下。

①绿色线条状态为：正在通讯中。

②暗蓝色线条状态为：通信中断。

③线条的粗细与流量的大小成正比。

④如果将鼠标移动至线条处，程序显示出流量双方位置、通讯流量的大小，并自动计算流量占当前网络的百分比。

02 单击【Matrix】（矩阵）对话框左下方的【IP】选项，则 Sniffer Pro 将以 IP 地址的形式表示捕捉到的网络主机，如图 7-59 所示。

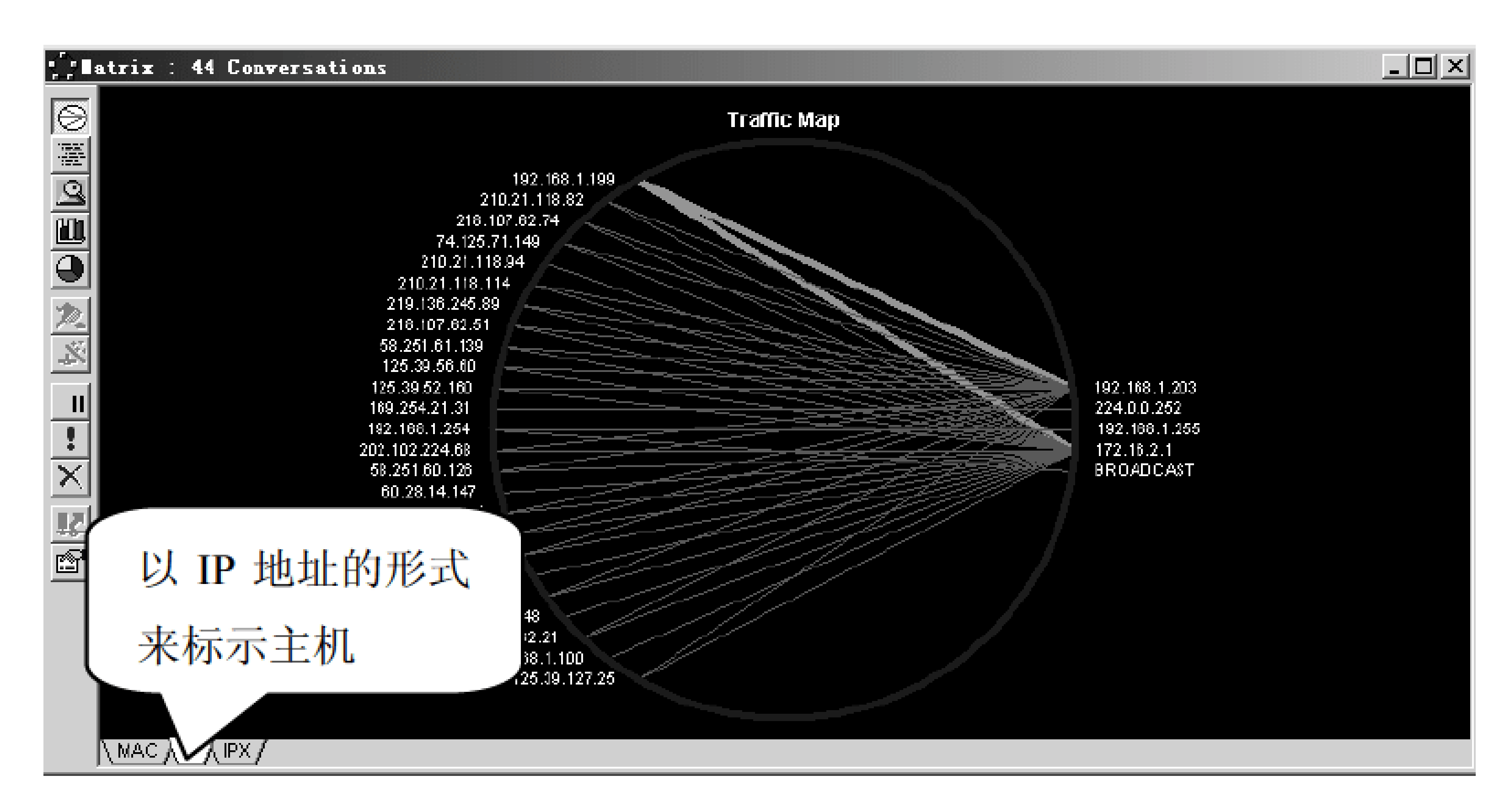


图 7-59

4. ART（应用响应时间）

ART（应用响应时间）主要用来显示网络中主机的上网行为，通过 ART（应用响应时间）可以看出网络主机的 HTTP 连接情况，可以直观看到网络用户正在浏览什么网站。

在 Sniffer Pro 的操作界面选择【Monitor】（监控）➢【Application Response Time】（应用响应时间）菜单命令，打开【Application Response Time】（应用响应时间）对话框，列出了网络主机正在使用 HTTP 协议和网络中的哪些主机进行通信，如图 7-60 所示。

Application Response Time (milliseconds) - HTTP: 14 Entries

Server Address	Client Address	AvgRsp	90%Rsp	MinRsp	MaxRsp	TotRsp	0-25	26-50	51-100	101-200	201-400	401-800	8(
116.255.136.105	howin-1f80af4ed	125	222	2	273	7	2	0	0	4	1	0	0
116.255.136.105	bogon	125	222	3	273	7	2	0	0	4	1	0	0
123.196.117.6	howin-1f80af4ed	68	99	3	217	11	2	1	7	0	1	0	0
123.196.117.6	bogon	69	99	3	217	11	2	1	7	0	1	0	0
216.218.207.147	howin-1f80af4ed	366	518	184	548	2	0	0	0	1	0	1	0
216.218.207.147	bogon	366	518	185	548	2	0	0	0	1	0	1	0
hx-in-f157.1e100.n	howin-1f80af4ed	97	173	3	191	2	1	0	0	1	0	0	0
hx-in-f157.1e100.n	bogon	98	173	4	192	2	1	0	0	1	0	0	0
hx-in-f166.1e100.n	howin-1f80af4ed	63	118	4	122	2	1	0	0	1	0	0	0
hx-in-f166.1e100.n	bogon	63	118	4	122	2	1	0	0	1	0	0	0
reverse.gdsz.cncn	howin-1f80af4ed	71	81	38	87	3	0	1	2	0	0	0	0
reverse.gdsz.cncn	bogon	71	82	39	87	3	0	1	2	0	0	0	0
60.28.14.147	howin-1f80af4ed	47	55	37	57	3	0	2	1	0	0	0	0
60.28.14.147	bogon	48	55	38	57	3	0	2	1	0	0	0	0

HTTP

图 7-60

5. Protocol Distribution（协议分类）

Protocol Distribution（协议分类）主要显示了网络中不同协议的使用情况，查看协议分类的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面选择【Monitor】（监控）➢【Protocol Distribution】（协议分类）菜单命令，打开【Protocol Distribution】（协议分类）窗口，用不同颜色显示了当前网络中不同协议的使用情况，如图 7-61 所示。

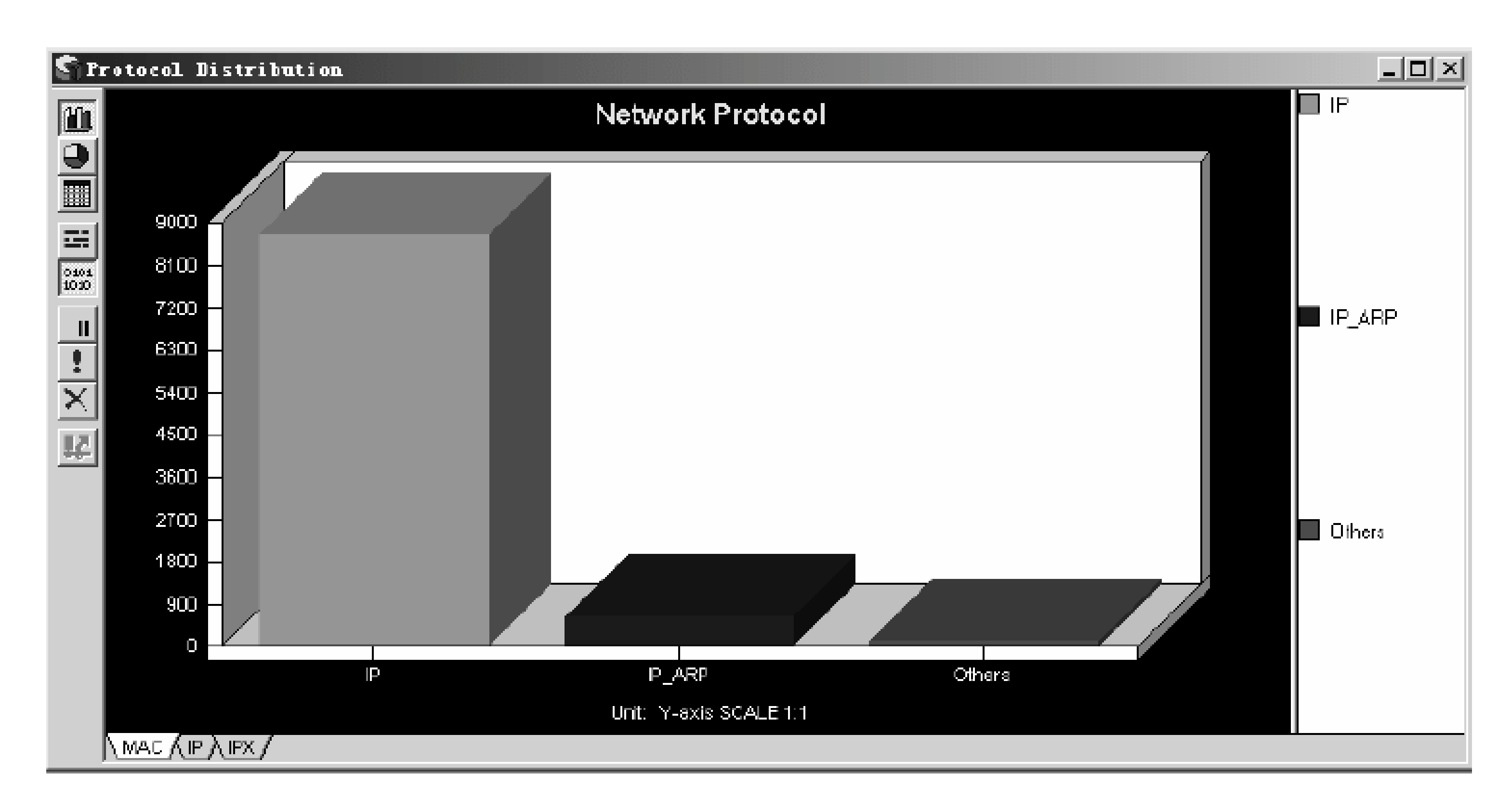


图 7-61

02 单击工具栏左侧【◕】图标，则将以饼形来显示不同协议的使用情况，如图 7-62 所示。

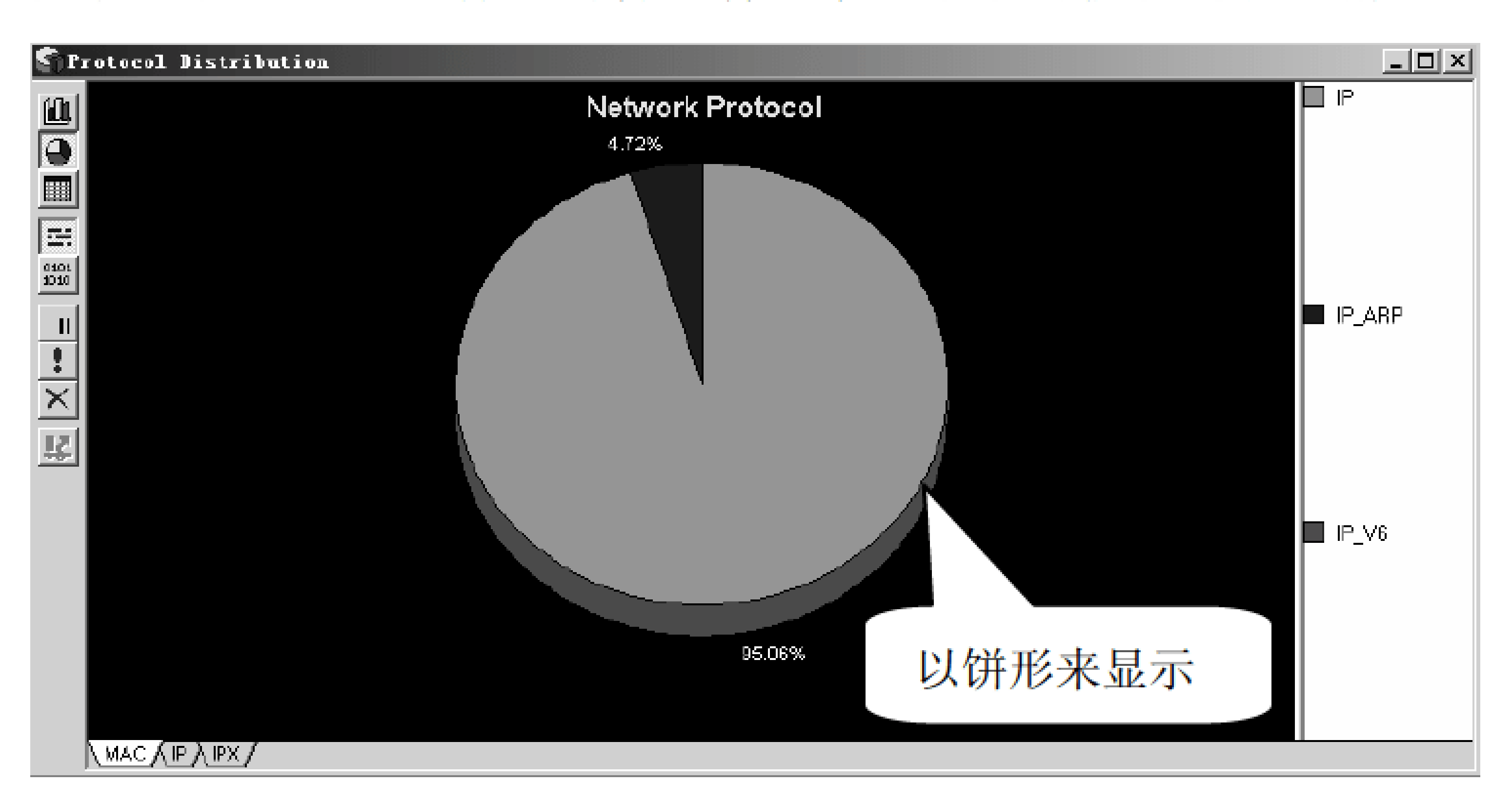


图 7-62

03 单击工具栏左侧【▦】图标，则将以表格的形式来显示不同协议的使用情况，如图 7-63 所示。

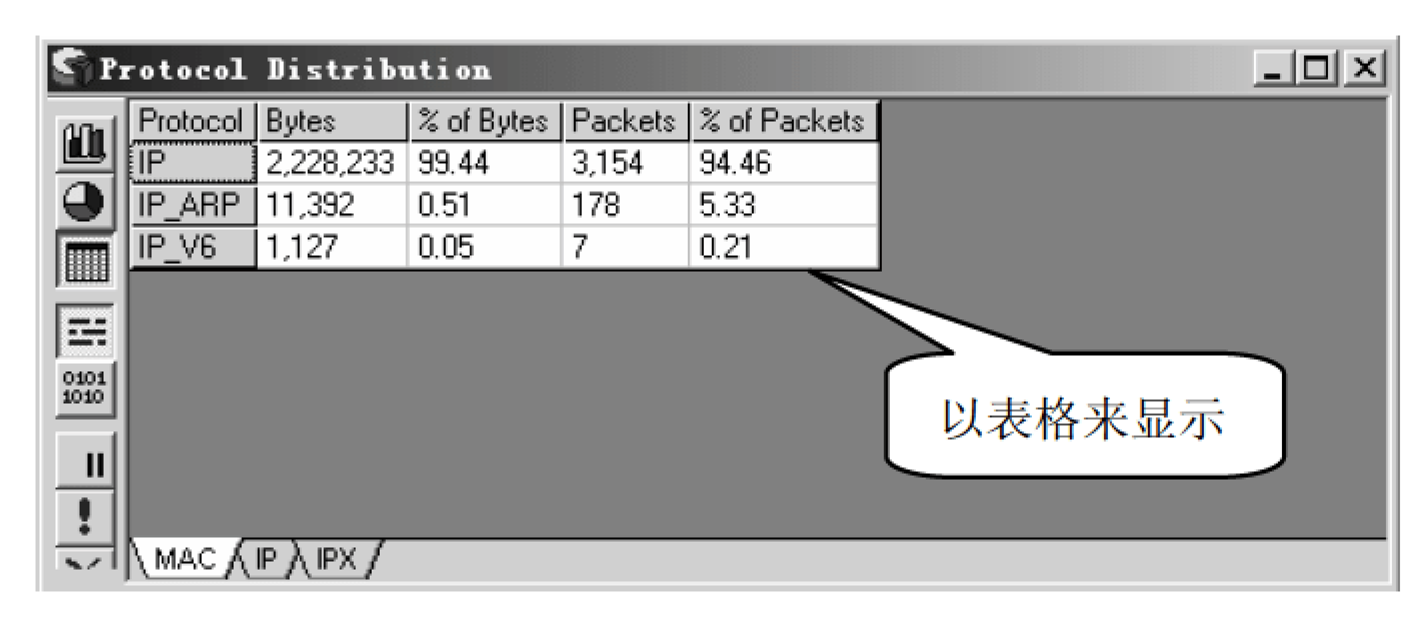


图 7-63

6. History Sample（历史采样）

History Sample（历史采样）可以捕捉到一段时间内各个阶段的网络利用情况。

在 Sniffer Pro 的操作界面中选择【Monitor】（监控）➢【History Sample】（历史采样）菜单命令，打开【History Sample】（历史采样）窗口，如图 7-64 所示。

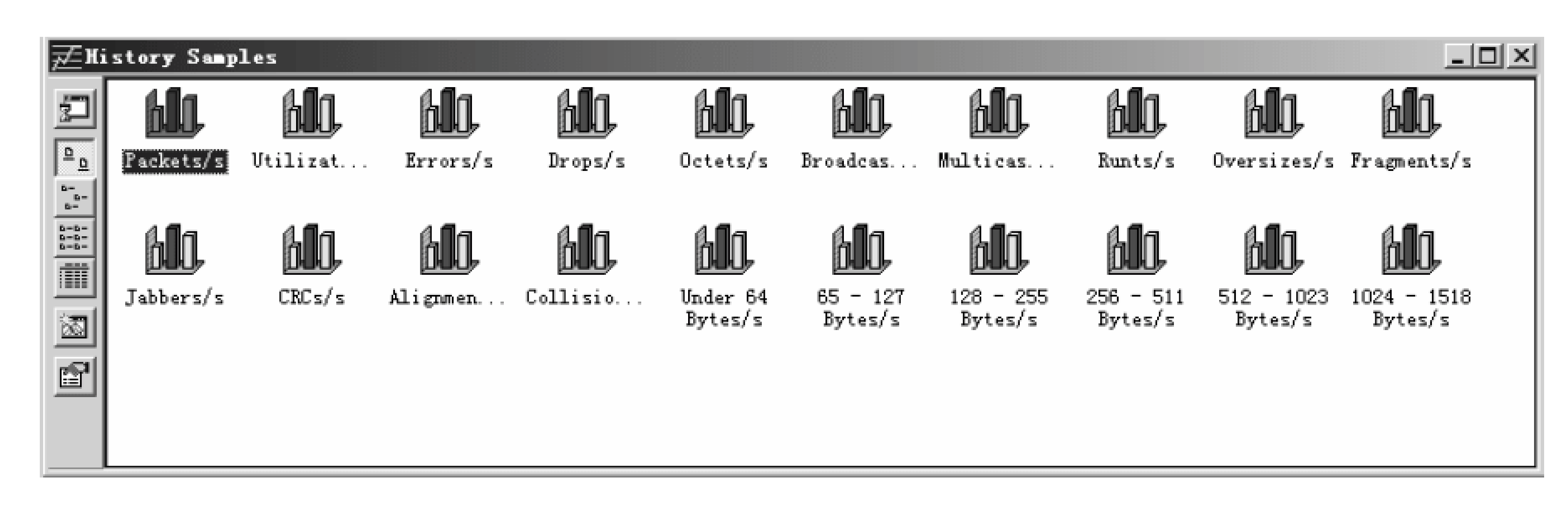


图 7-64

如果想看网络中这一时段每秒钟传输的数据包，双击【】图标，弹出【Packets/s】（每秒的数据包数量）对话框。在【Packets/s】（每秒的数据包数量）对话框下方的时间表明捕捉的是什么时间段的数据包，History Sample（历史采样）每隔 15 秒捕捉一次。管理员可以将这个记录进行保存，以便日后分析网络时使用，如图 7-65 所示。

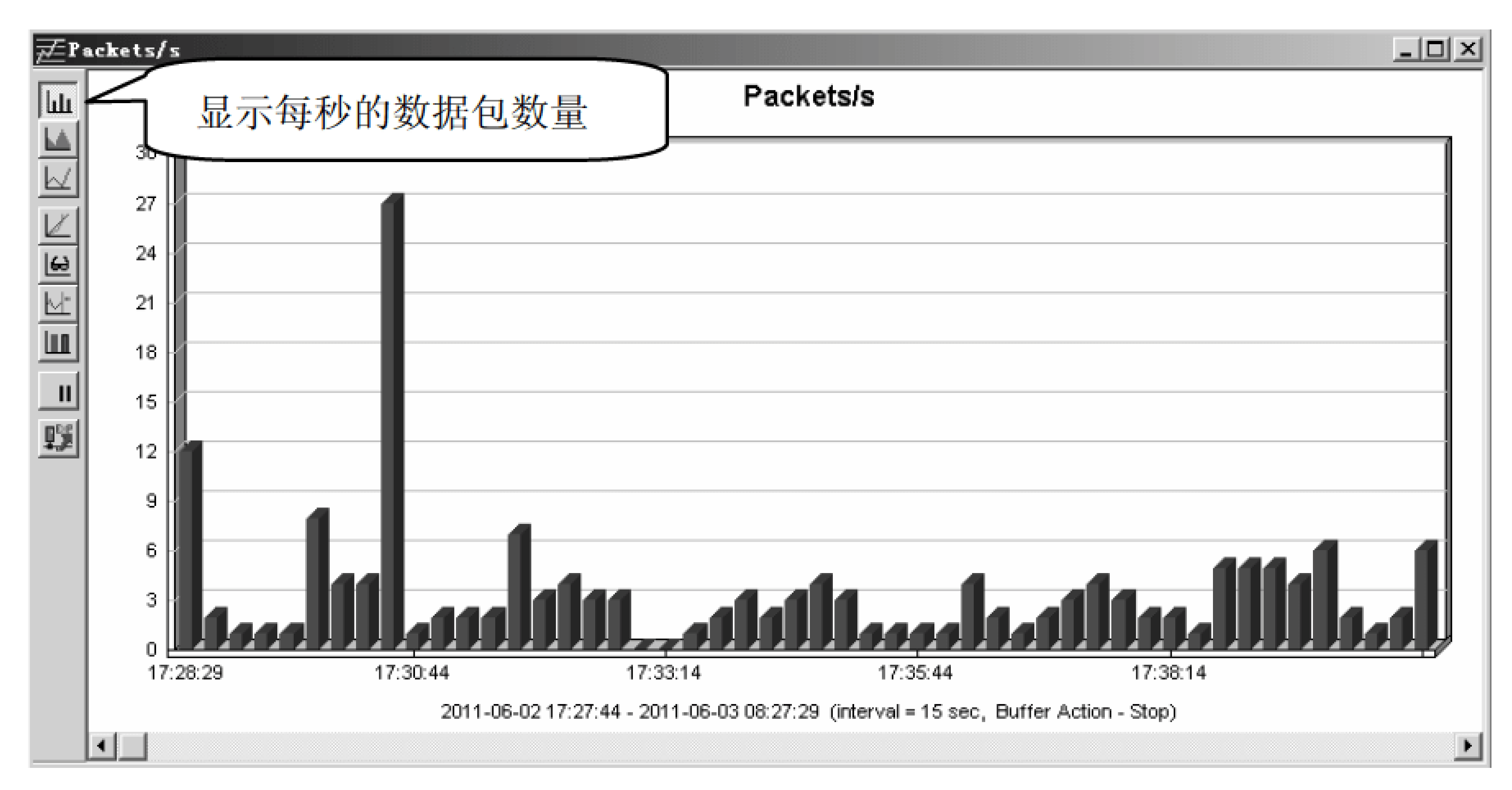


图 7-65

7. Global Statistics（全局统计）

Global Statistics（全局统计）用来显示网络中传输的数据包大小分布。

在 Sniffer Pro 的操作界面中选择【Monitor】（监控）➢【Global Statistics】（全局统计）菜单命令，打开【Global Statistics】（全局统计）对话框。如图 7-66 所示，在其中可以查看全局统计信息。

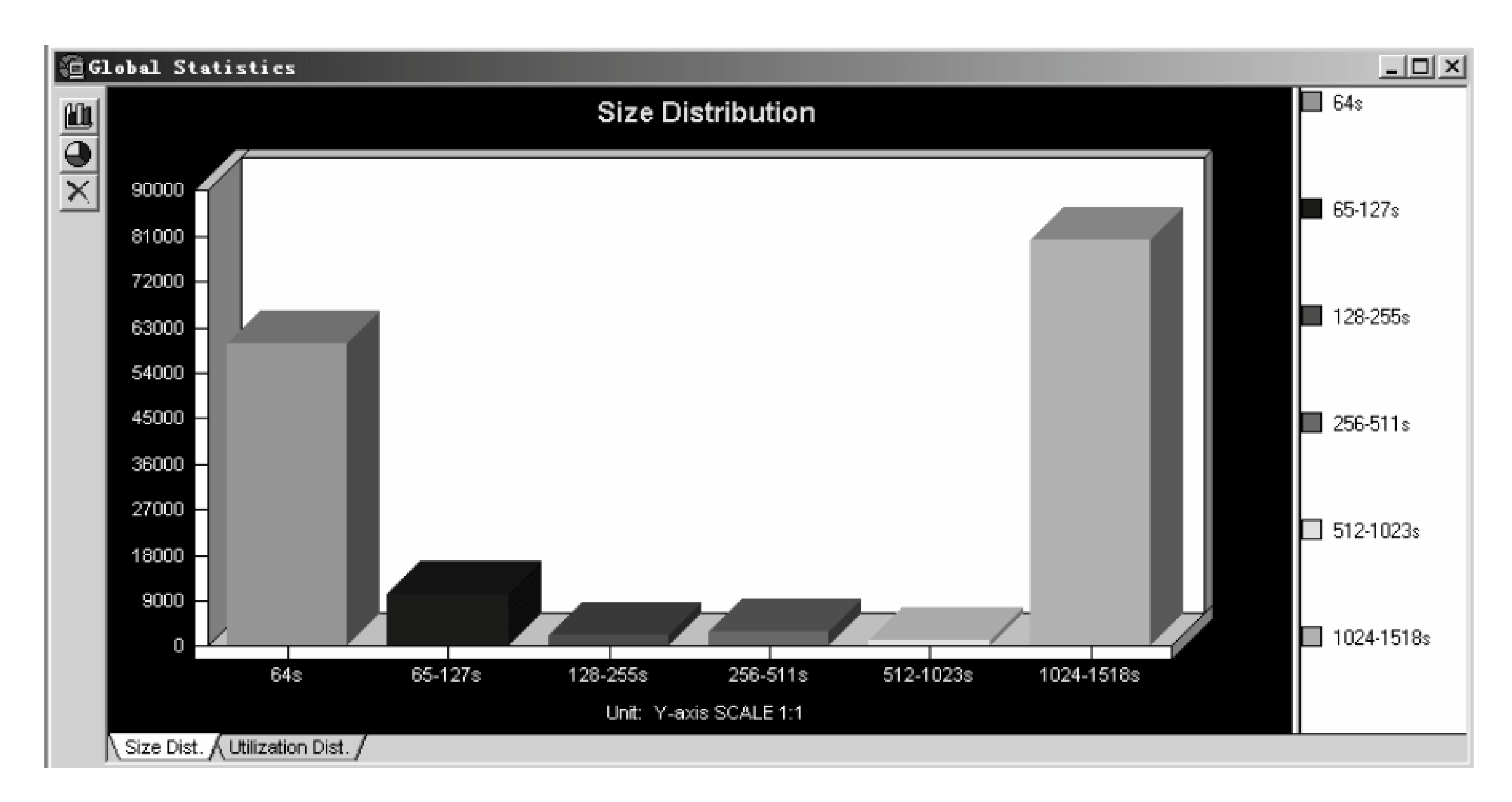


图 7-66

7.4.4　捕捉数据包

默认情况下，Sniffer Pro 会监听所有的数据包，在实际的数据包捕获过程中，有些数据是无关紧要的，如特定主机的数据包、符合某种网络协议的数据包等。这时就需要设置捕捉数据包的过滤条件，Sniffer 只捕捉与条件相关的数据包，这样可以大大节省分析数据包的时间。

1. 设置 IP 过滤规则

通过添加一个过滤器，使得 Sniffer Pro 只捕捉特定 IP 地址段的数据包，具体操作步骤如下。

01 在 Sniffer Pro 的操作界面中选择【Capture】（捕获）➢【Define Filer】（定义过滤器）菜单命令，弹出【Define Filter – Capture】（定义捕获过滤器）对话框，单击【Profiles】（配置文件）按钮，如图 7-67 所示。

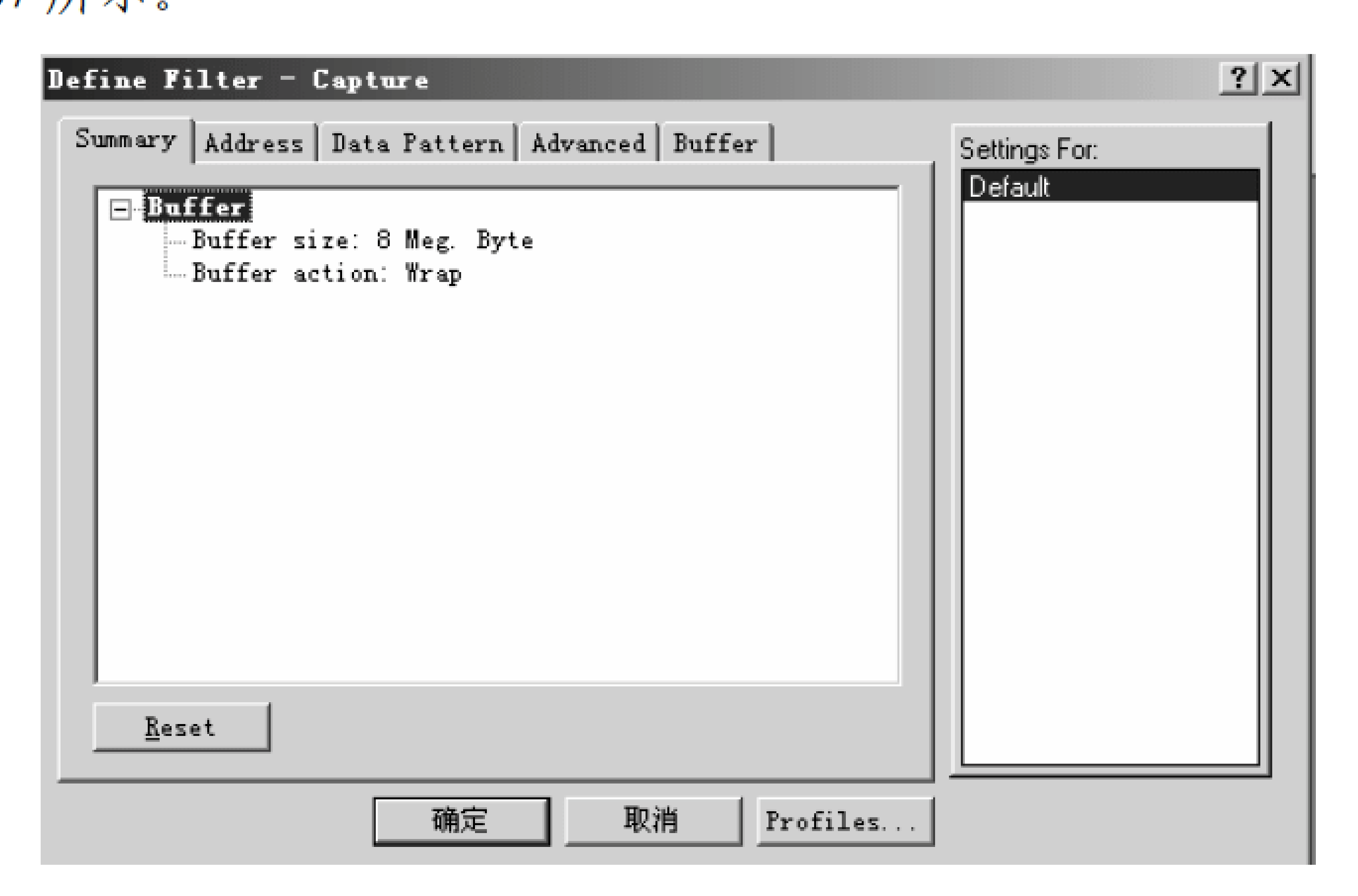


图 7-67

02 弹出【Capture Profiles】（捕捉配置文件）对话框，单击【New】（新建）按钮，如图 7-68 所示。

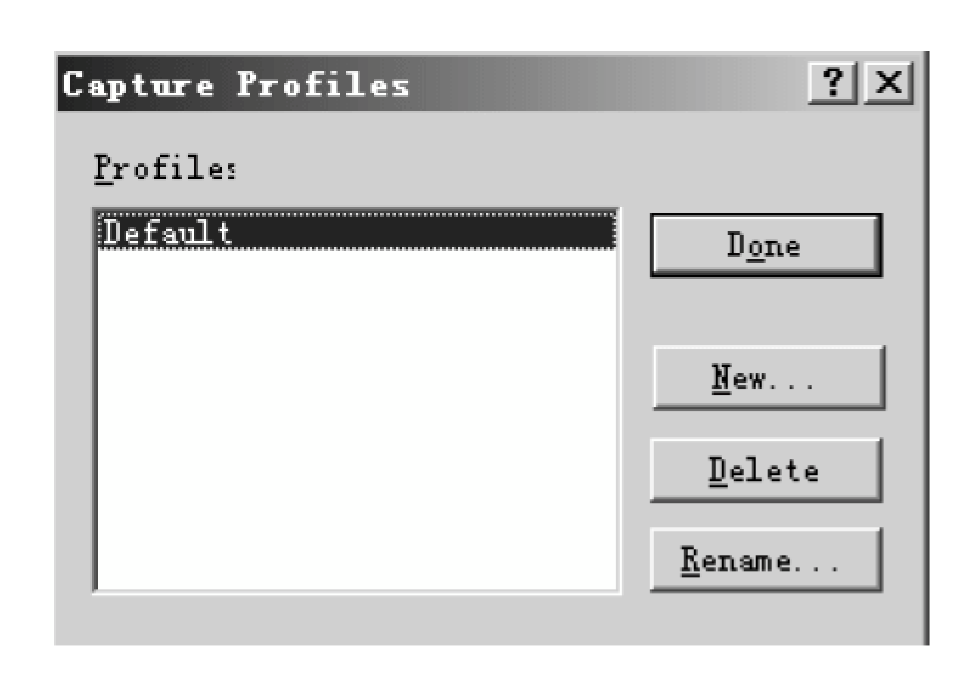


图 7-68

03 弹出【New Capture Profile】（新的捕捉配置文件）对话框，在【New Profile Name】（新的配置文件名字）文本框输入过滤器的名字，单击【OK】（确定）按钮，一个新的过滤器创建完成，如图 7-69 所示。

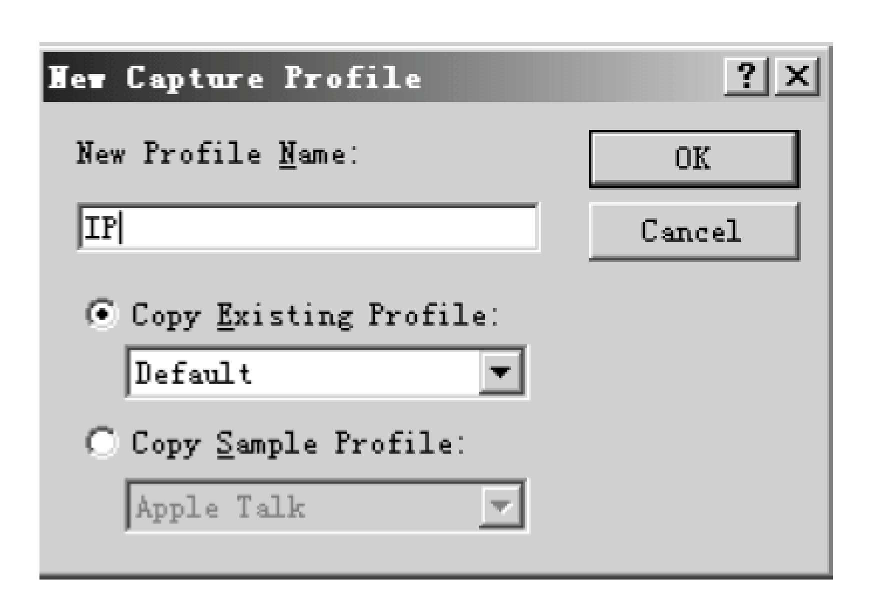


图 7-69

04 返回至【Capture Profiles】（捕捉配置文件）对话框，单击【Done】（是）按钮，如图 7-70 所示。

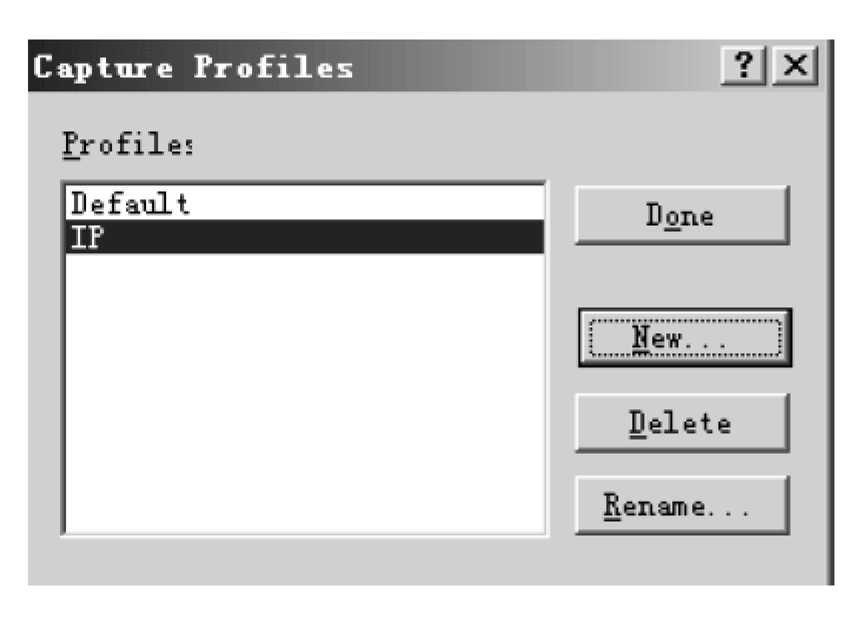


图 7-70

05 返回【Define Filter – Capture】（捕捉过滤器）对话框，选择【Address】（地址）选项卡，在【Address】（地址）下拉列表中选择【IP】选项，如图 7-71 所示。

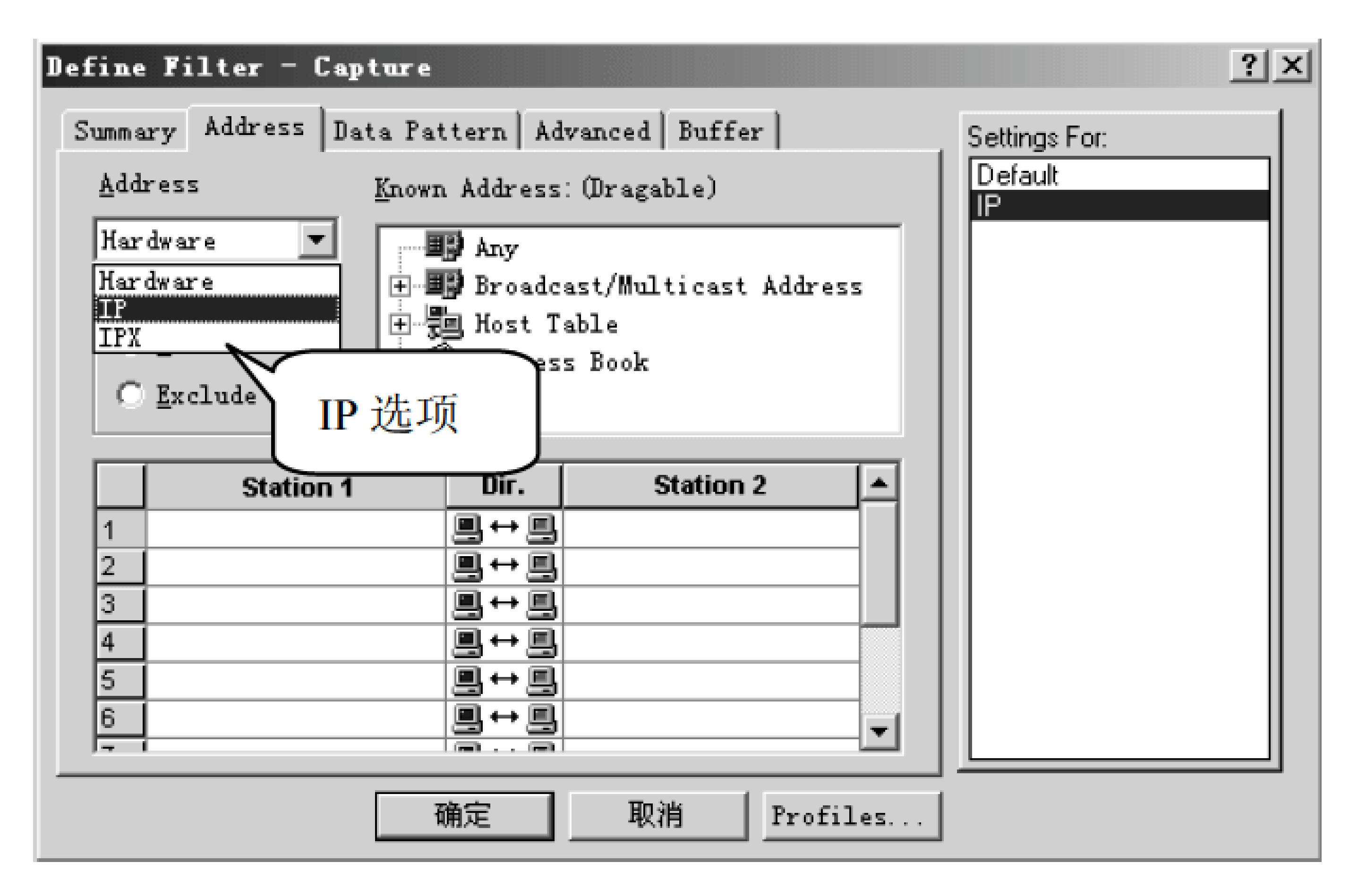


图 7-71

06 在【Station 1】（起始地址）和【Station 2】（结束地址）文本框中分别输入要捕捉的 IP 地址范围，本实例输入 172.16.4.1 至 172.16.4.3，单击【确定】按钮，则一个新的 IP 过滤器创建完成，如图 7-72 所示。

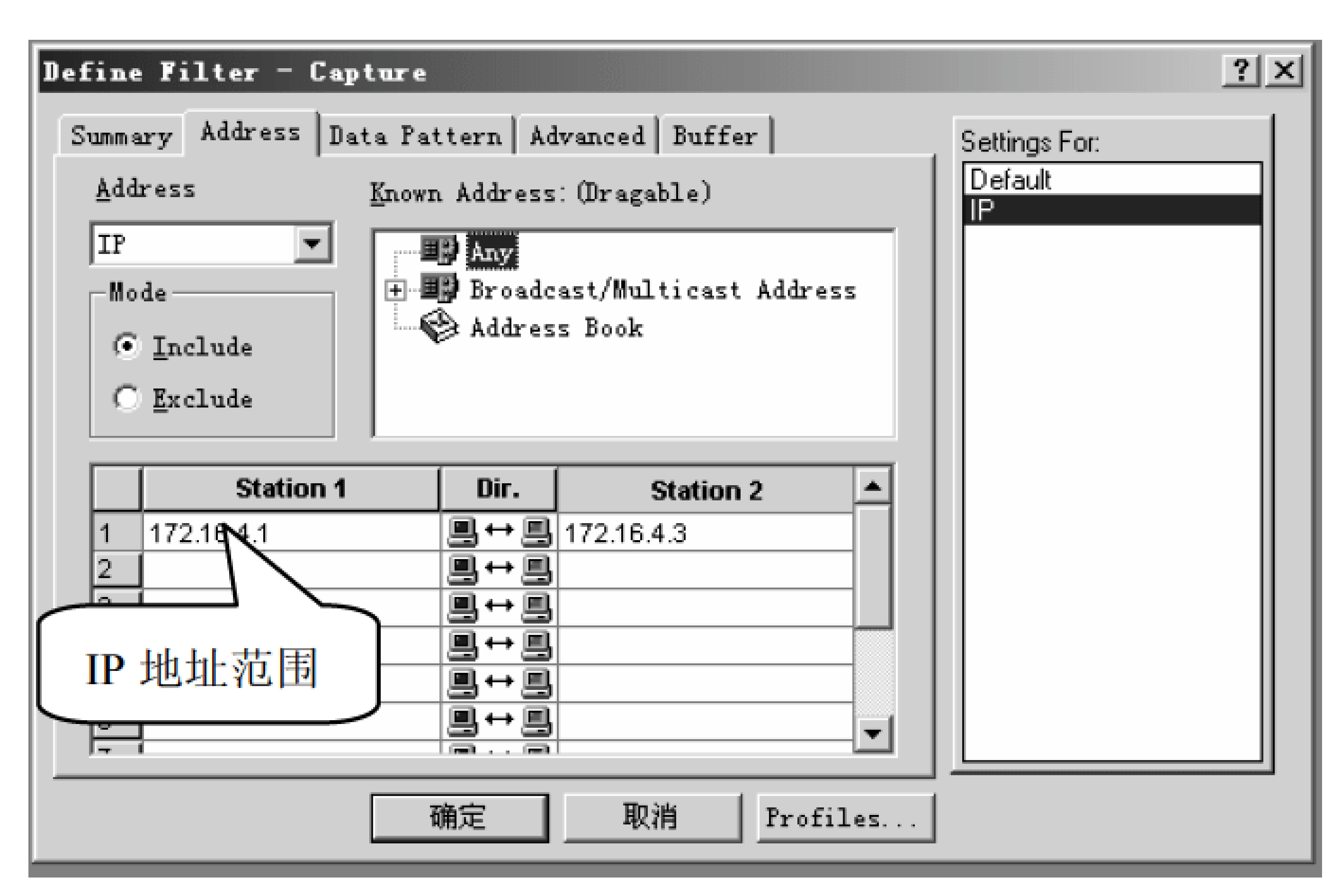


图 7-72

2. 设置协议过滤规则

网络通信过程中都需要用到各种各样的网络协议，在监听数据的时候，在 Sniffer Pro 中可以设置只监听某个协议或者某些协议的通信信息。

设置过滤器过滤与特定通信协议相关的数据包具体操作步骤如下。

01 在 Sniffer Pro 的操作界面中选择【Capture】（捕捉）➢【Define Filer】（定义过滤器）菜单命令，弹出【Define Filter – Capture】（定义捕捉过滤器）对话框，单击【Profiles】（配置文件）按钮，如图 7-73 所示。

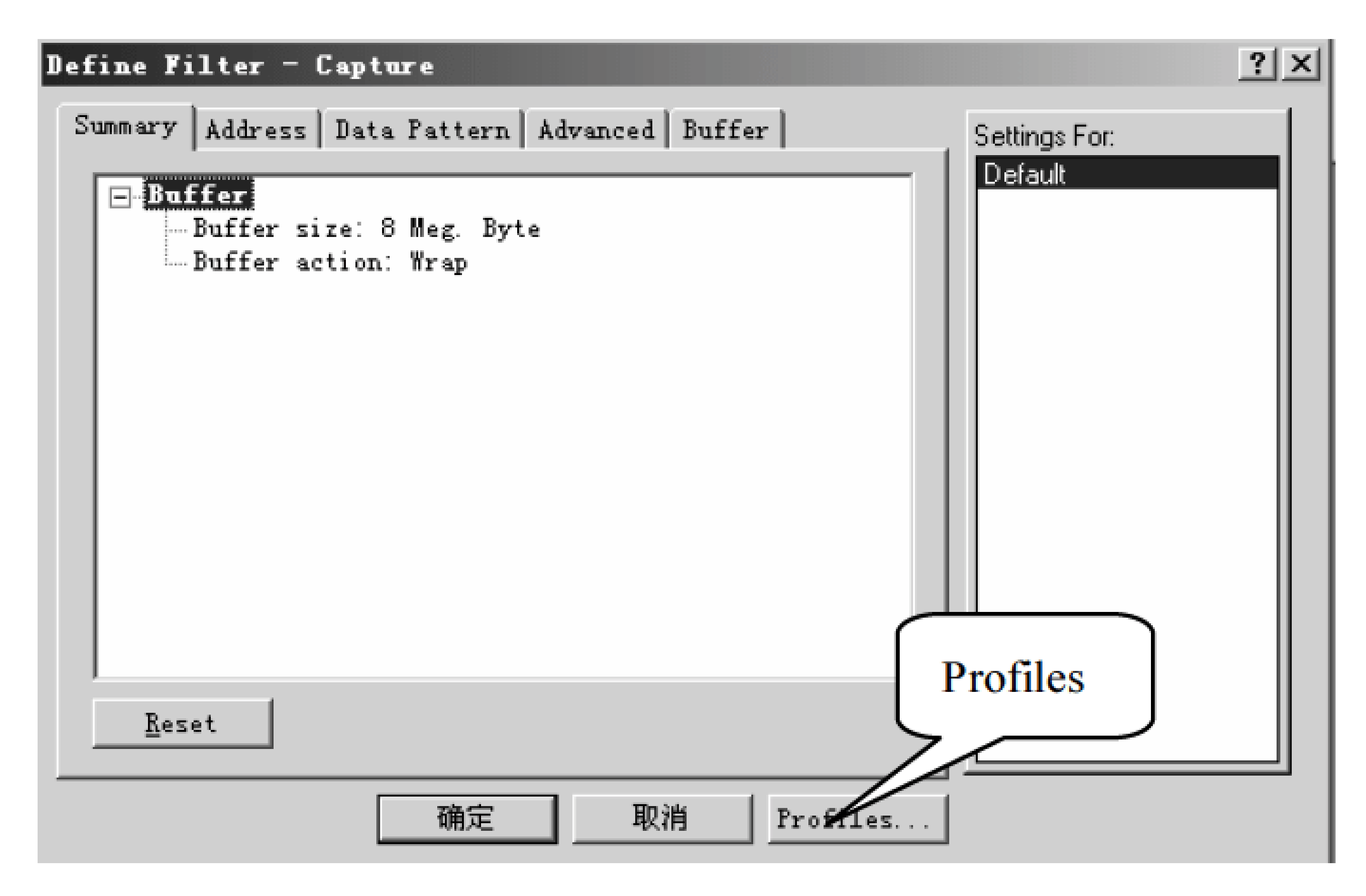


图 7-73

02 弹出【Capture Profiles】（捕捉配置文件）对话框，单击【New】（新建）按钮，如图 7-74 所示。

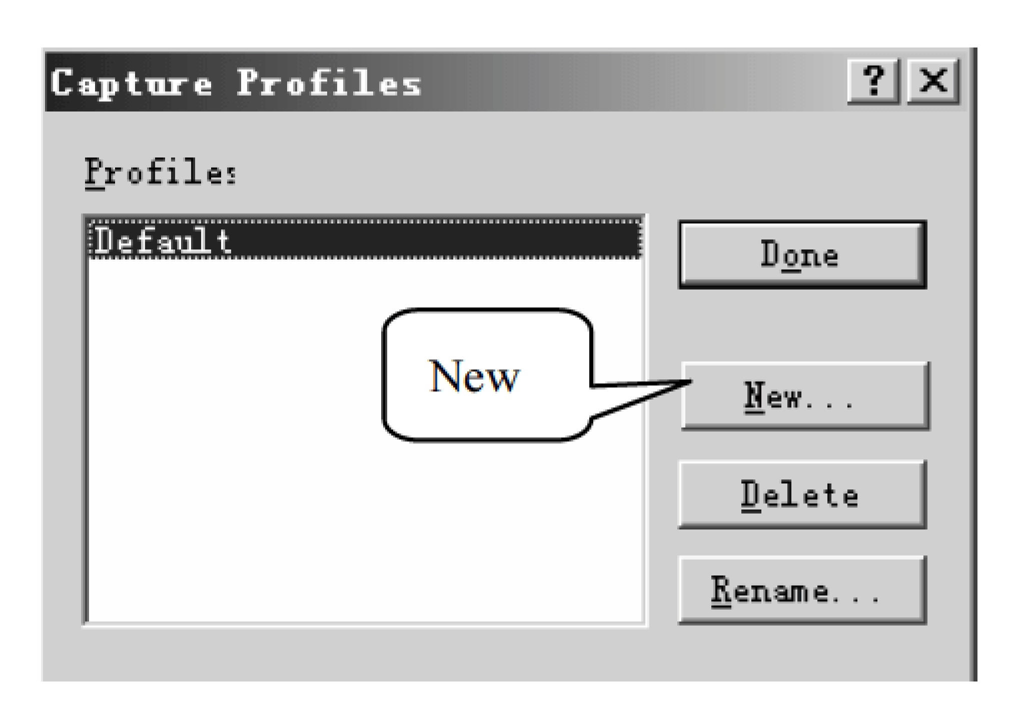


图 7-74

03 弹出【New Capture Profile】（新的捕捉配置文件）对话框，在【New Profile Name】（新的配置文件名字）文本框输入过滤器的名字“protocol”，单击【OK】（确定）按钮，一个新的过滤器创建完成，如图 7-75 所示。

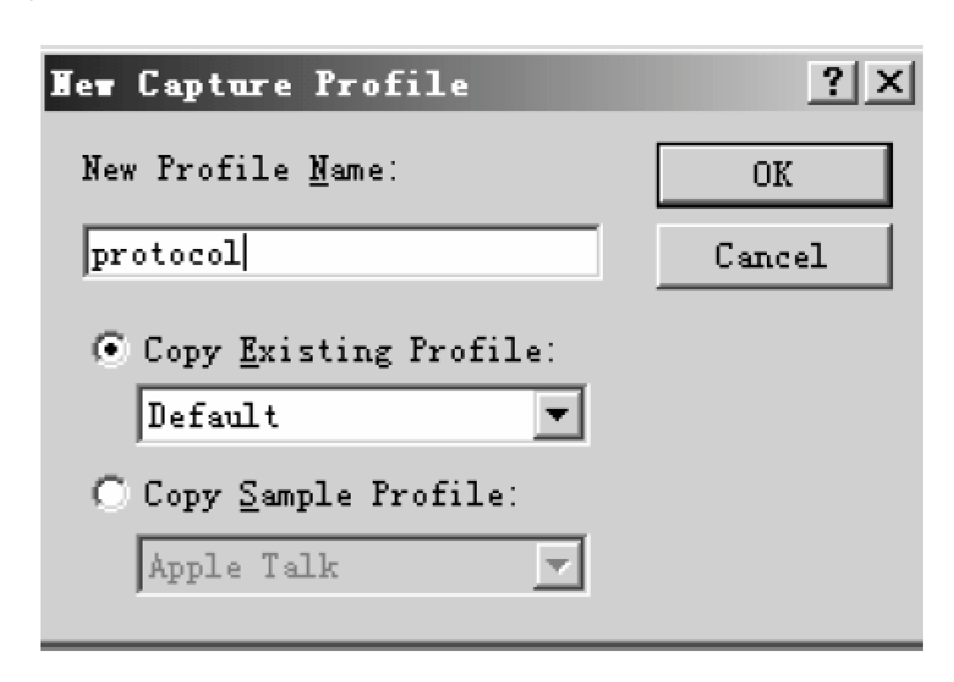


图 7-75

04 返回至【Capture Profiles】（捕捉配置文件）对话框，单击【Done】（是）按钮，如图 7-76 所示。

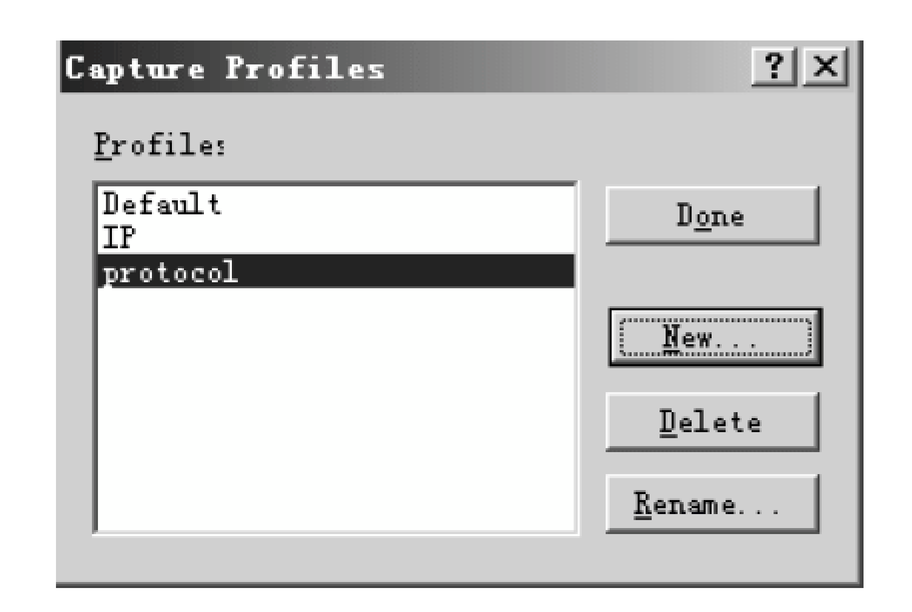


图 7-76

05 返回【Define Filter – Capture】（捕捉过滤器）对话框，选择【Advanced】（高级）选项卡，选择【IP】➢【TCP】➢【FTP】选项，单击【确定】按钮，一个新的网络协议过滤器创建完成，如图 7-77 所示。

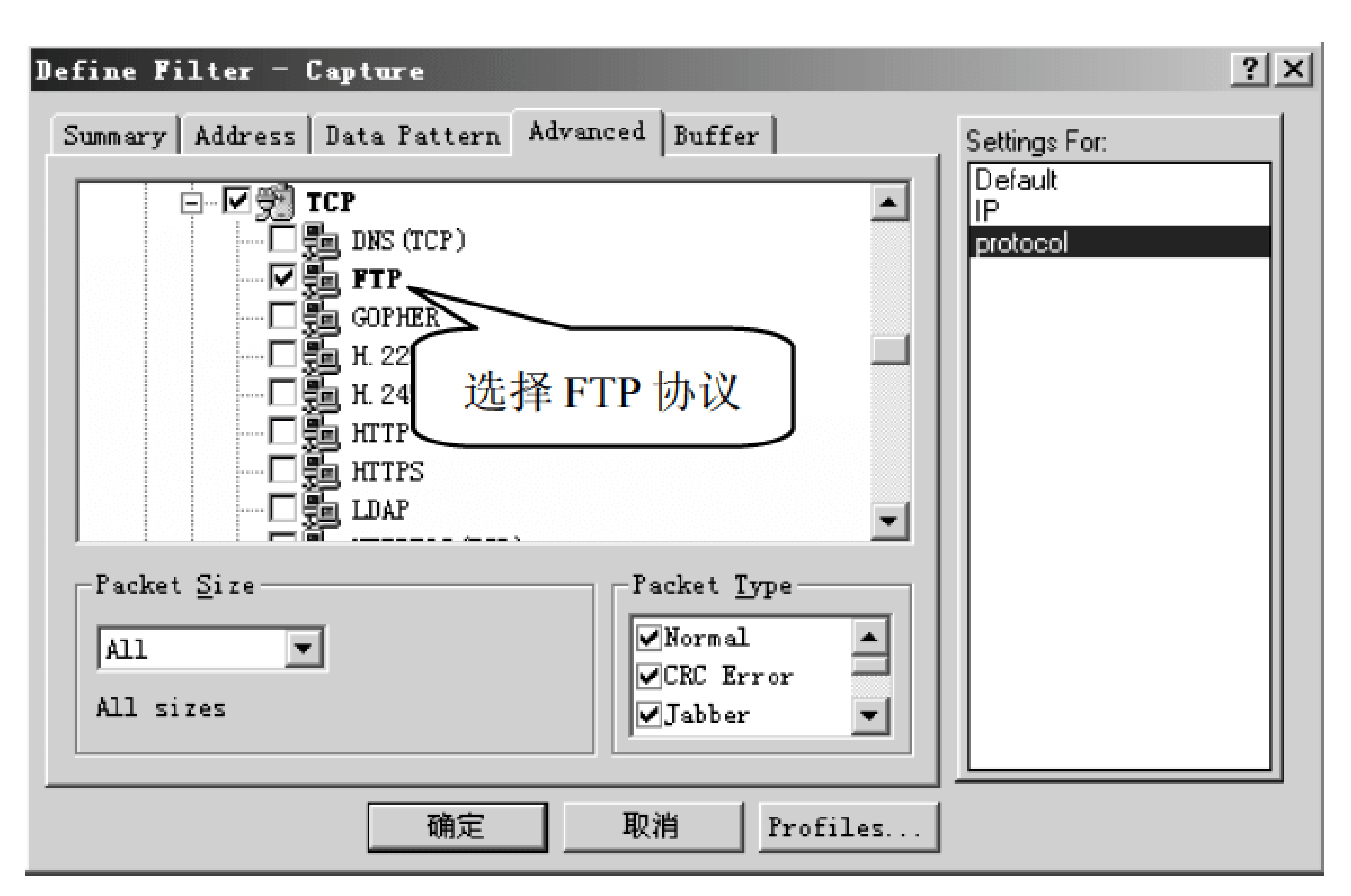


图 7-77

默认情况下，Sniffer Pro 会捕捉所有经过 Sniffer 监听网卡的数据包，网络管理员可以对这些数据进行分析，从而发现网络存在的问题。

3. 选择合适的过滤器

在 Sniffer Pro 的操作界面中选择【Capture】（捕捉）➢【Define Filer】（定义过滤器）菜单命令，弹出【Define Filter – Capture】（定义捕捉过滤器）对话框，单击【Settings For】（设置）文本框下面要使用的过滤器 Default，单击【确定】按钮，如图 7-78 所示。

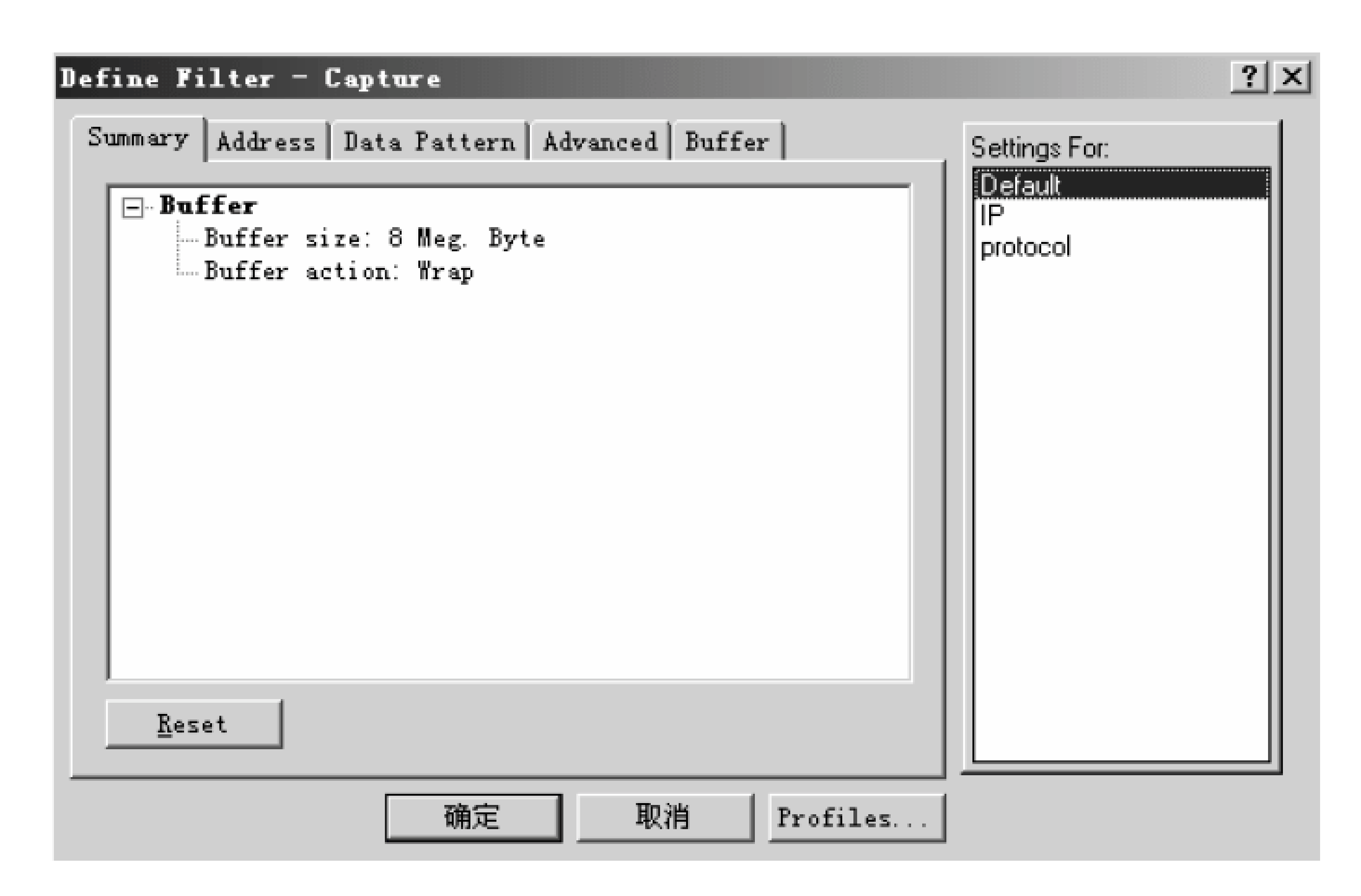


图 7-78

4. 捕捉数据包

具体的操作步骤如下。

01 选择【Capture】（捕捉）➢【start】（开始）菜单命令，或者单击工具栏上的【▶】按钮开始数据包捕捉，弹出【Expert】（专家）窗口，如图 7-79 所示。

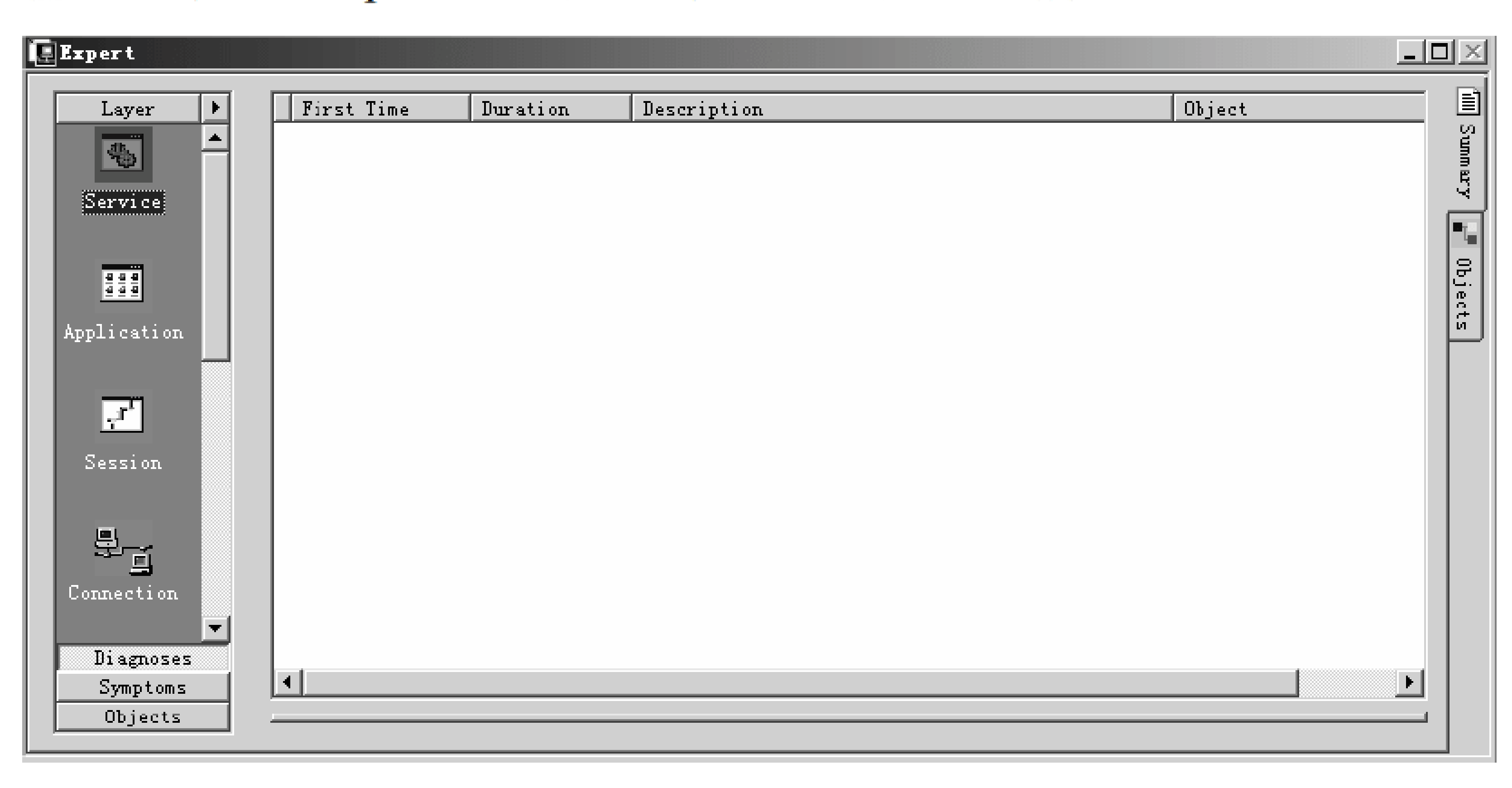


图 7-79

02 当数据包捕捉包完毕后，选择【Capture】（捕捉）➢【stop and display】（停止并显示）菜单命令，或者单击工具栏上的【▣】按钮，弹出如图 7-80 所示的【snif2: Expert,105 unknown frames】（105 个未知的帧）窗口。

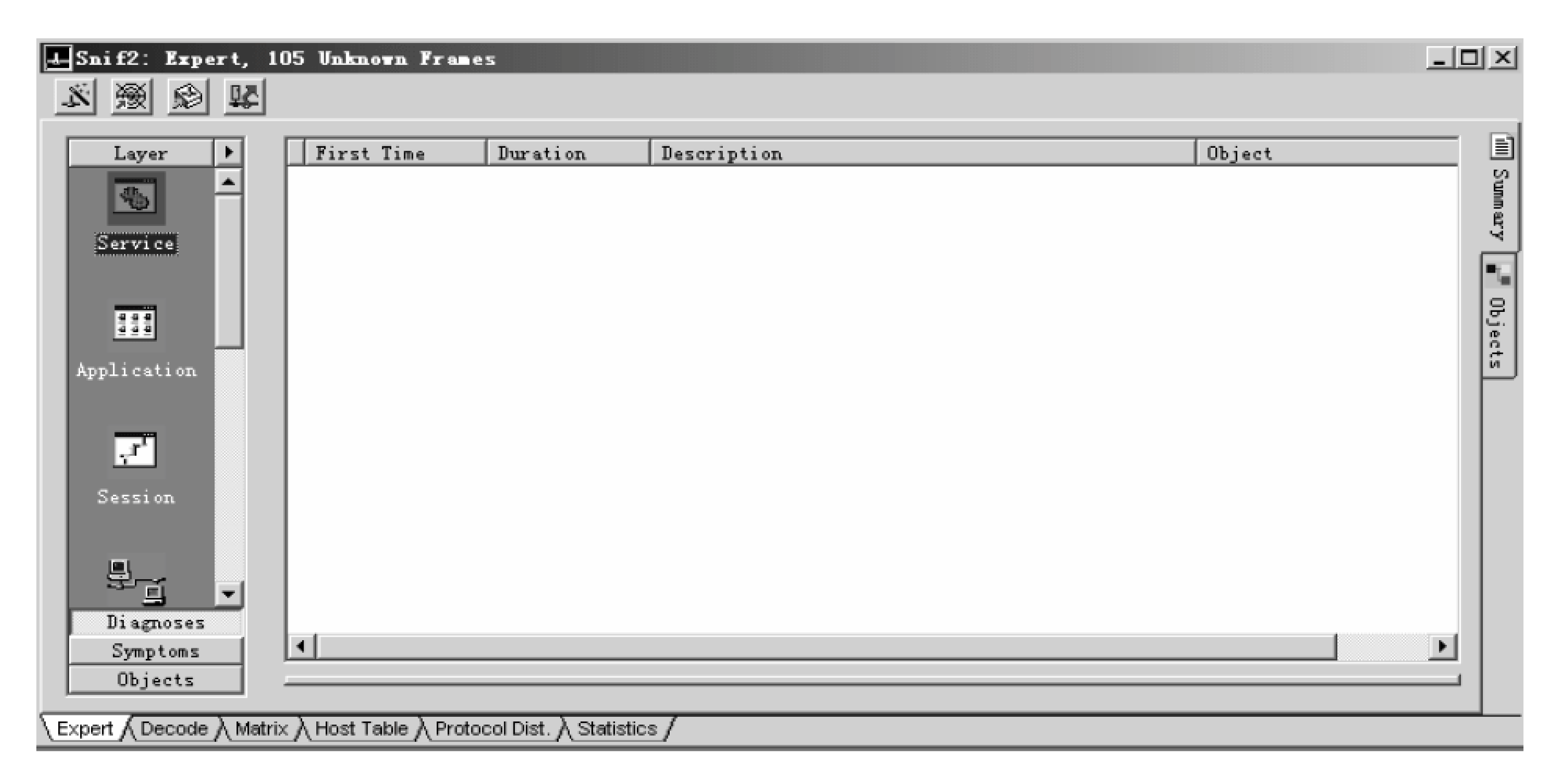


图 7-80

03 单击下面的【Decode】(解码)按钮，进入 Sniffer 的专家解码系统，在其中可以查看相关的数据信息，如图 7-81 所示。

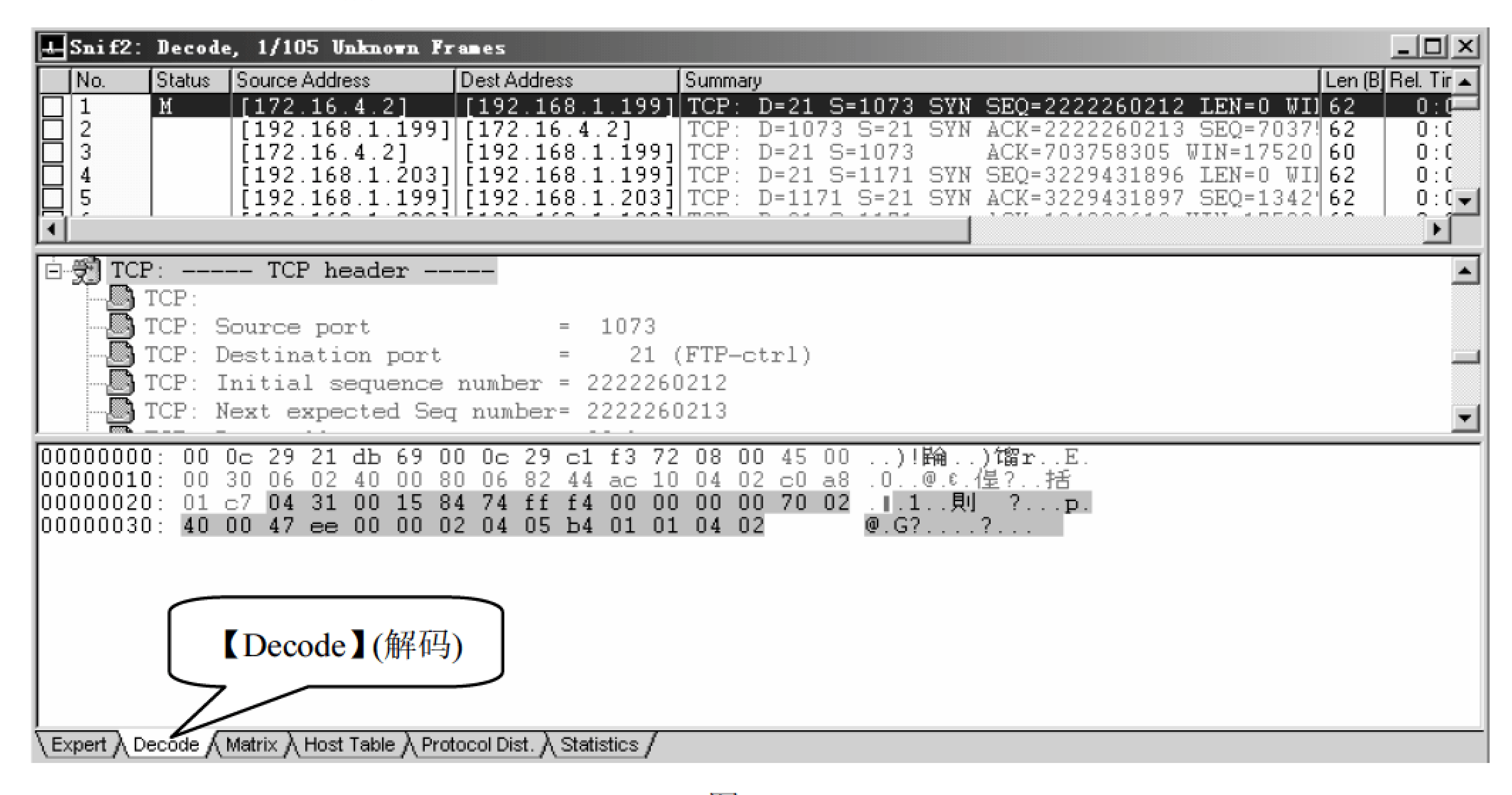


图 7-81

5. 分析捕捉到的数据包

在 Sniffer Pro 的专家解码界面中，主要分为三部分，从上往下分别是捕捉到的数据包、详细资料、包的十六进制数据信息。

分析捕获到的数据包的具体操作步骤如下。

01 在捕获的数据信息中选择需要分析的数据包信息，如图 7-82 所示为 FTP 数据包。

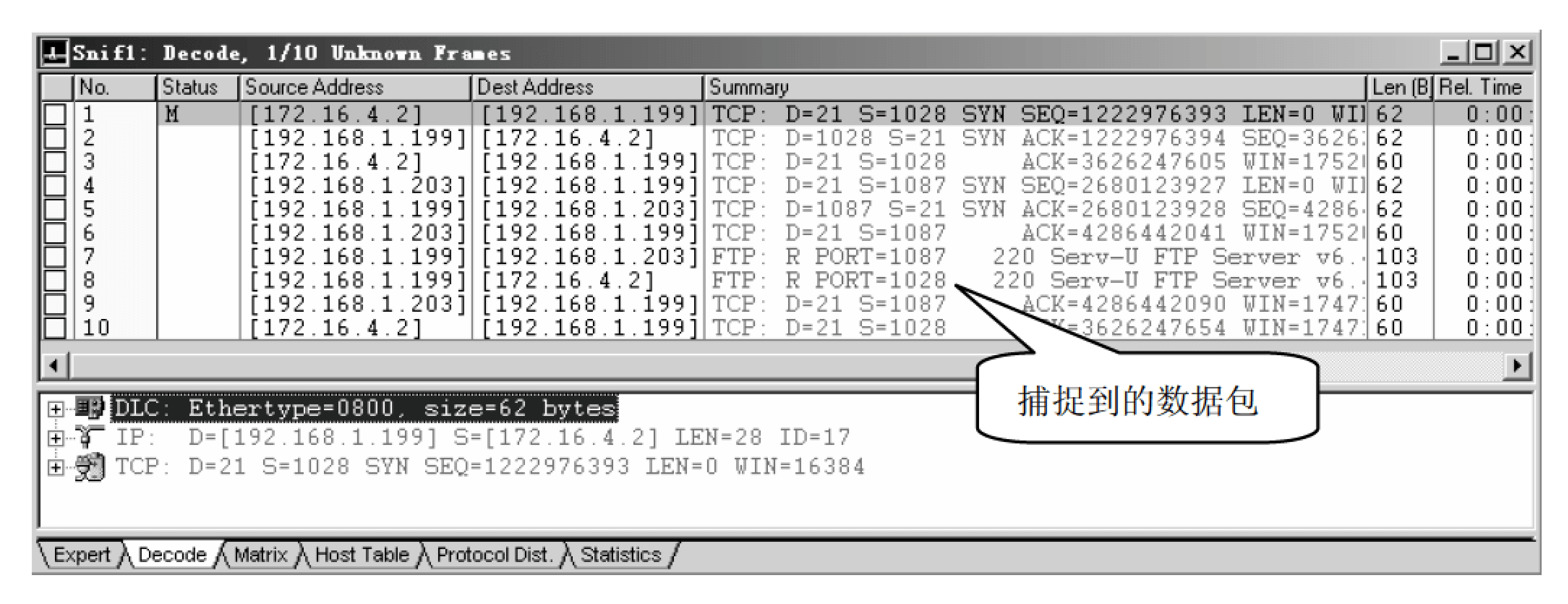


图 7-82

窗口中的相关参数含义如下。

- 【No】(序列号): 捕捉到的数据包的序列号。
- 【Status】(状态):捕捉到的数据包的状态。
- 【Source Address】(源地址): 捕捉到的数据包的源地址。
- 【Dest Address】(目标地址): 捕捉到的数据包的目标地址。
- 【Summary】(总结): 捕捉到的数据包的总结信息。

02 单击【DLC】前面的【+】号按钮，展开【DLC】(数据链路控制)模块，在【DLC】(数据链路控制)区域中显示了捕捉的帧的数据链路层信息，如图 7-83 所示。

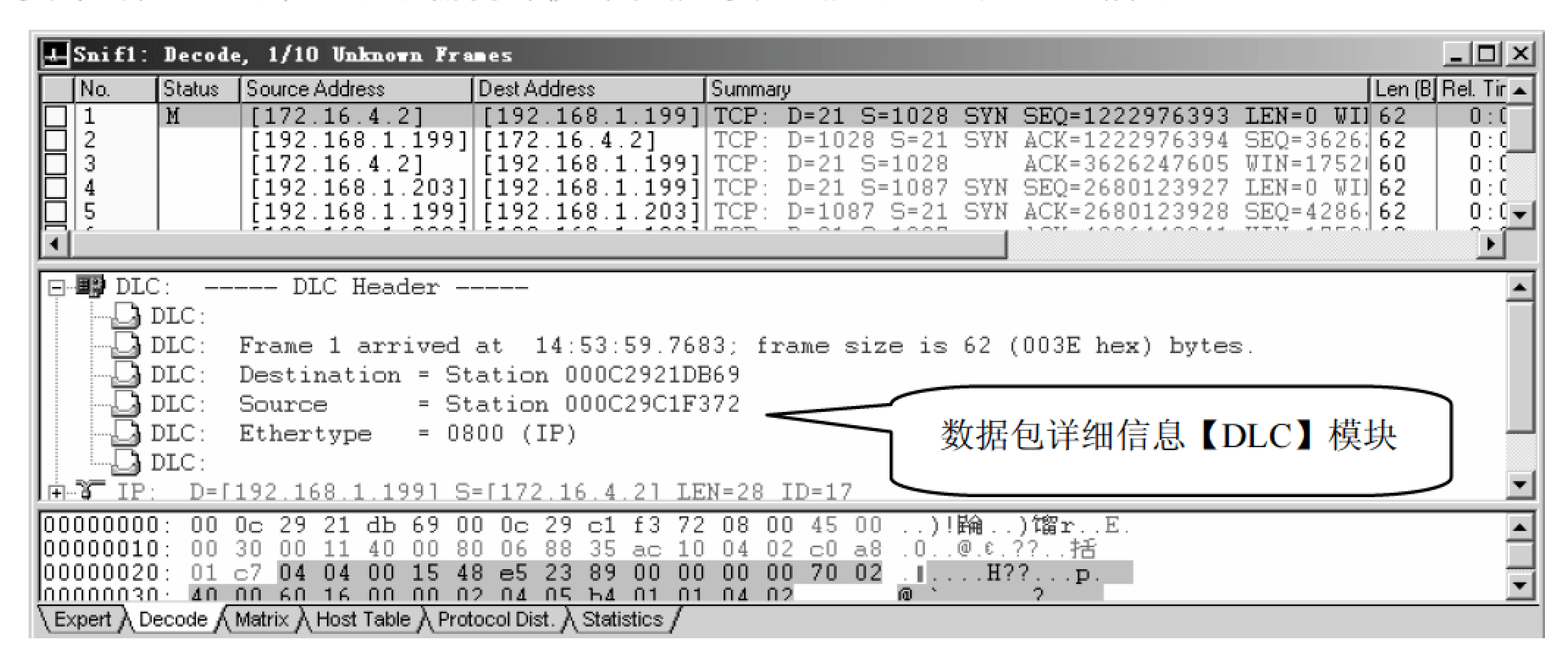


图 7-83

主要包括以下内容。

- 【Destination】(目的物理地址): 捕捉到的数据的目的物理地址。
- 【Source】(源物理地址): 捕捉到的数据包的源物理地址。
- 【Ethertype】(以太类型): 在这里以太类型为 0800，表示是 IPv4。

03 单击【IP】前面的【+】号按钮，展开【IP】模块，在【IP】区域中主要显示了捕捉到的数据包的网络层信息，如图 7-84 所示。

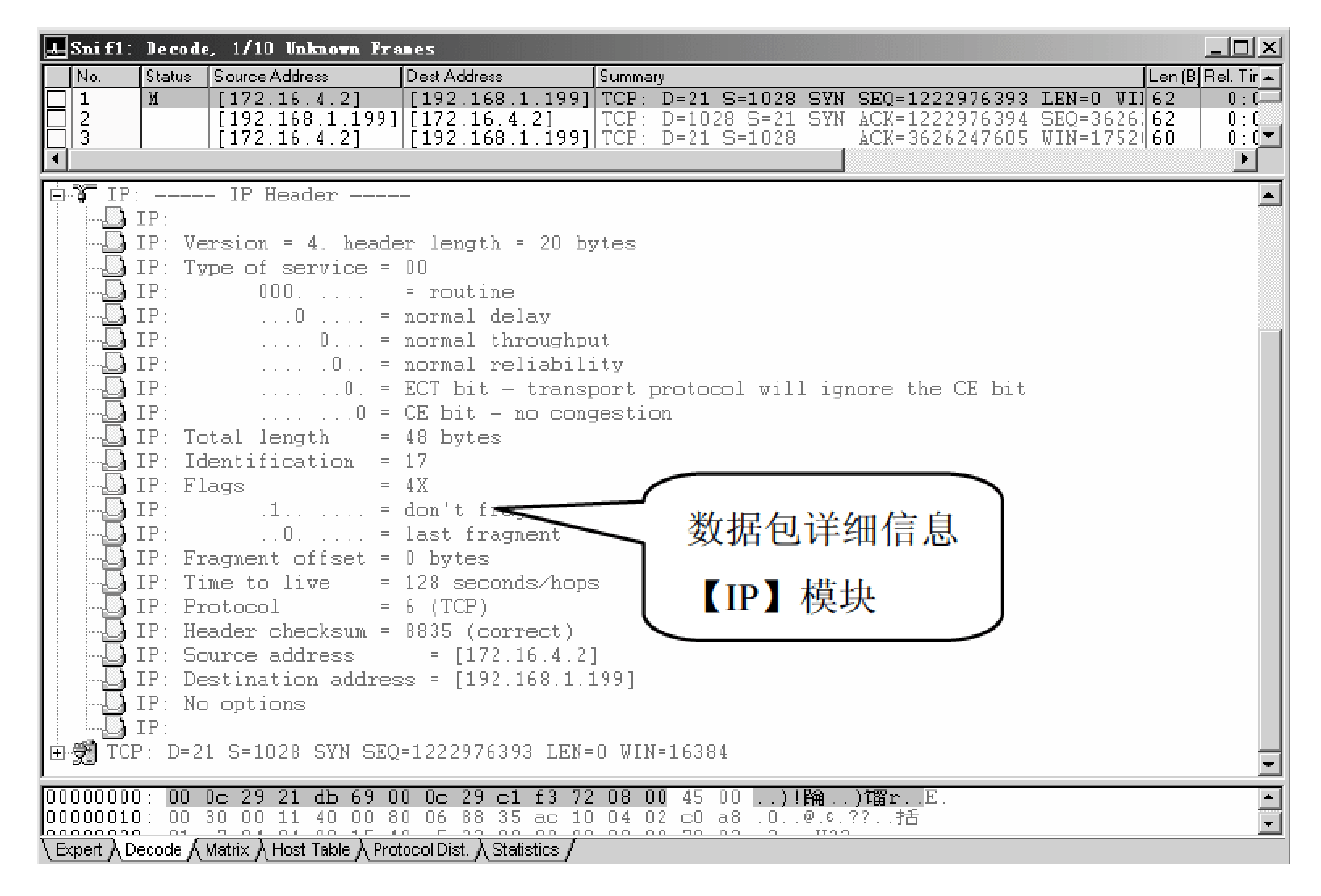


图 7-84

主要包括以下内容。

- 【Version】(版本)：IP 协议的版本，4 表示 IPv4，6 表示 IPv6。
- 【Total length】(总长度)：IP 数据包的总长度。
- 【Time to live】(保存时间)：表示 TTL 值的大小，说明一个数据包保存时间的长短。
- 【Protocol】(协议)：这个数据包上一层使用什么协议，这里的上一层是传输层，用的是 TCP 协议。
- 【Source address】(源地址)：数据包的源 IP 地址。
- 【Destination address】(目标地址)：数据包的目标 IP 地址。

04 单击【TCP】前面的【+】号，展开【TCP】模块，在【TCP】区域中主要显示了捕捉到得数据包的传输层的相关信息，如图 7-85 所示。

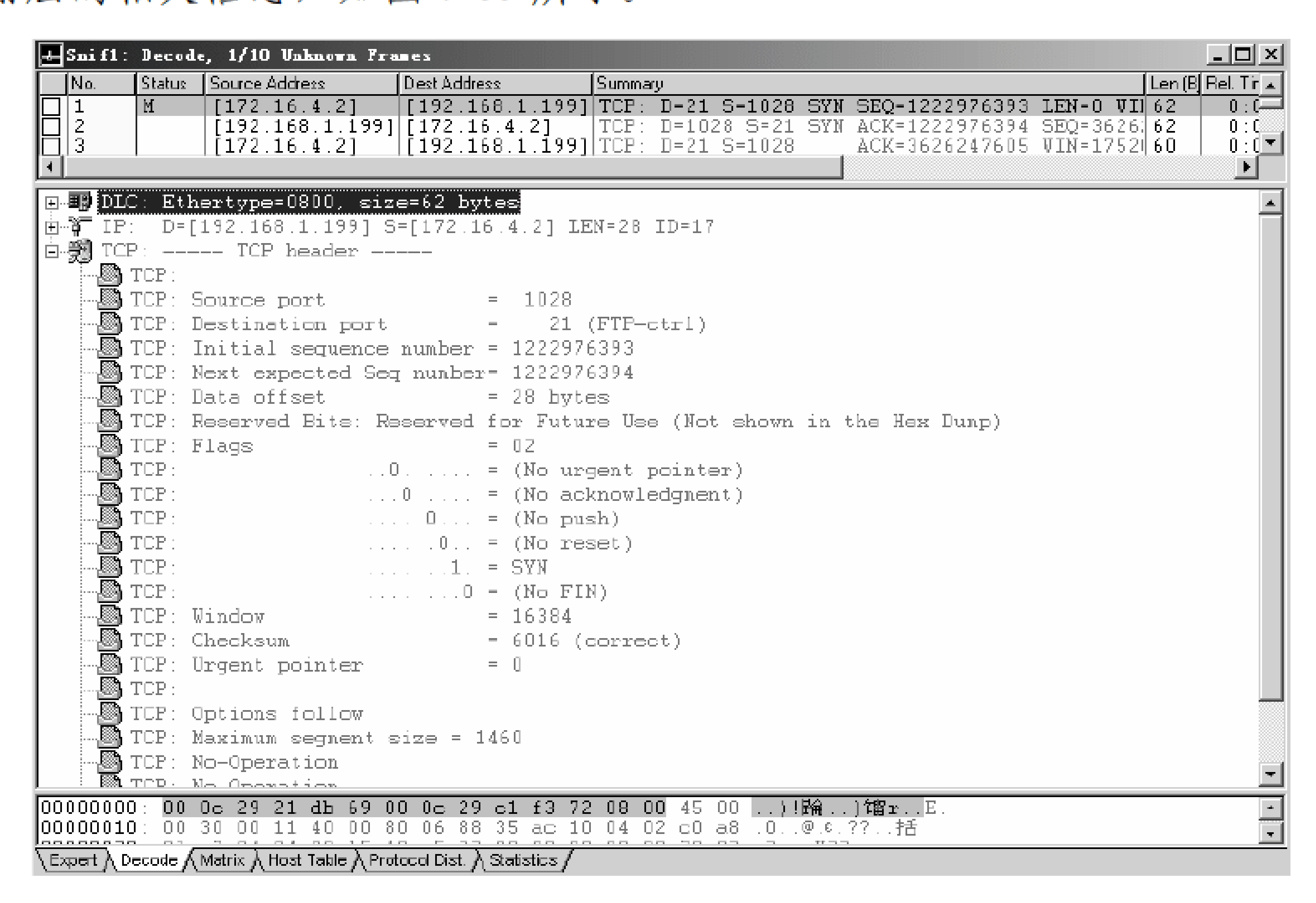


图 7-85

主要包括以下内容。

- 【Source port】(源端口)：数据包在传输层使用 TCP 源端口号。
- 【Destination port】(目标端口)：数据包在传输层使用 TCP 目标端口号。
- 【Checksum】(校验和)：显示了 TCP 协议的校验和。

05 单击窗口下方【Matrix】（矩阵）按钮，可以直观的显示网络中各计算机之间的链接，如图 7-86 所示。

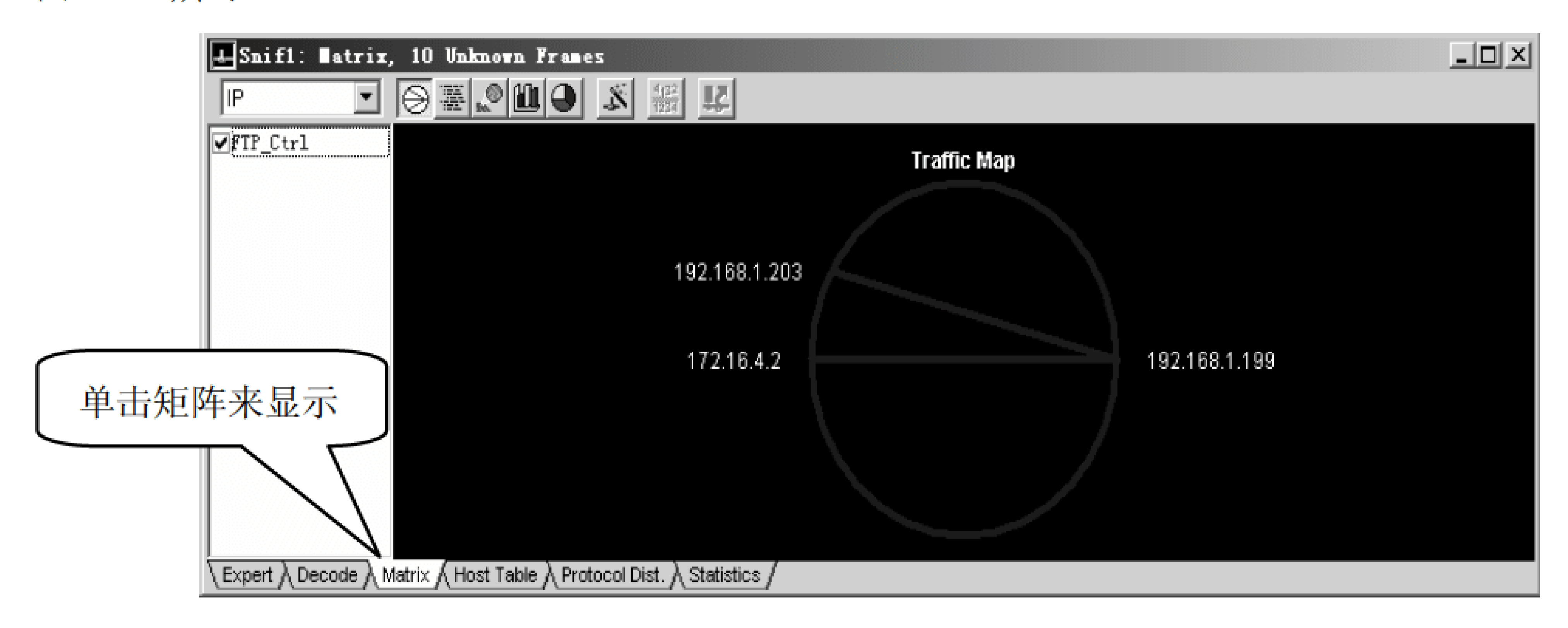


图 7-86

06 对于捕捉到的数据包，为了便于日后查询或者是比较使用，往往需要保存。当捕捉结束后，在 Sniffer Pro 主操作界面中选择【File】➢【Save】选项，即可将当前已捕捉到的数据包保存在硬盘中。

6. 使用 Sniffer Pro 分析客户端登陆 FTP 的过程

网络管理员经常会面临着在企业防火墙中设置如何允许内网主机访问部分外网服务，或者是禁止内网主机访问外网的某个服务的情况，这时就需要详细了解服务的运行信息。Sniffer Pro 可以帮助管理员快速的掌握某项服务的数据包的实际流动信息。

下面介绍客户机登陆外网 FTP 服务器时的数据包流动情况，具体操作步骤如下。

01 单击 Sniffer Pro 操作界面中工具栏上的【▶】按钮，开始捕捉数据包，如图 7-87 所示，然后在客户机中的一台电脑上登陆 FTP 服务器。

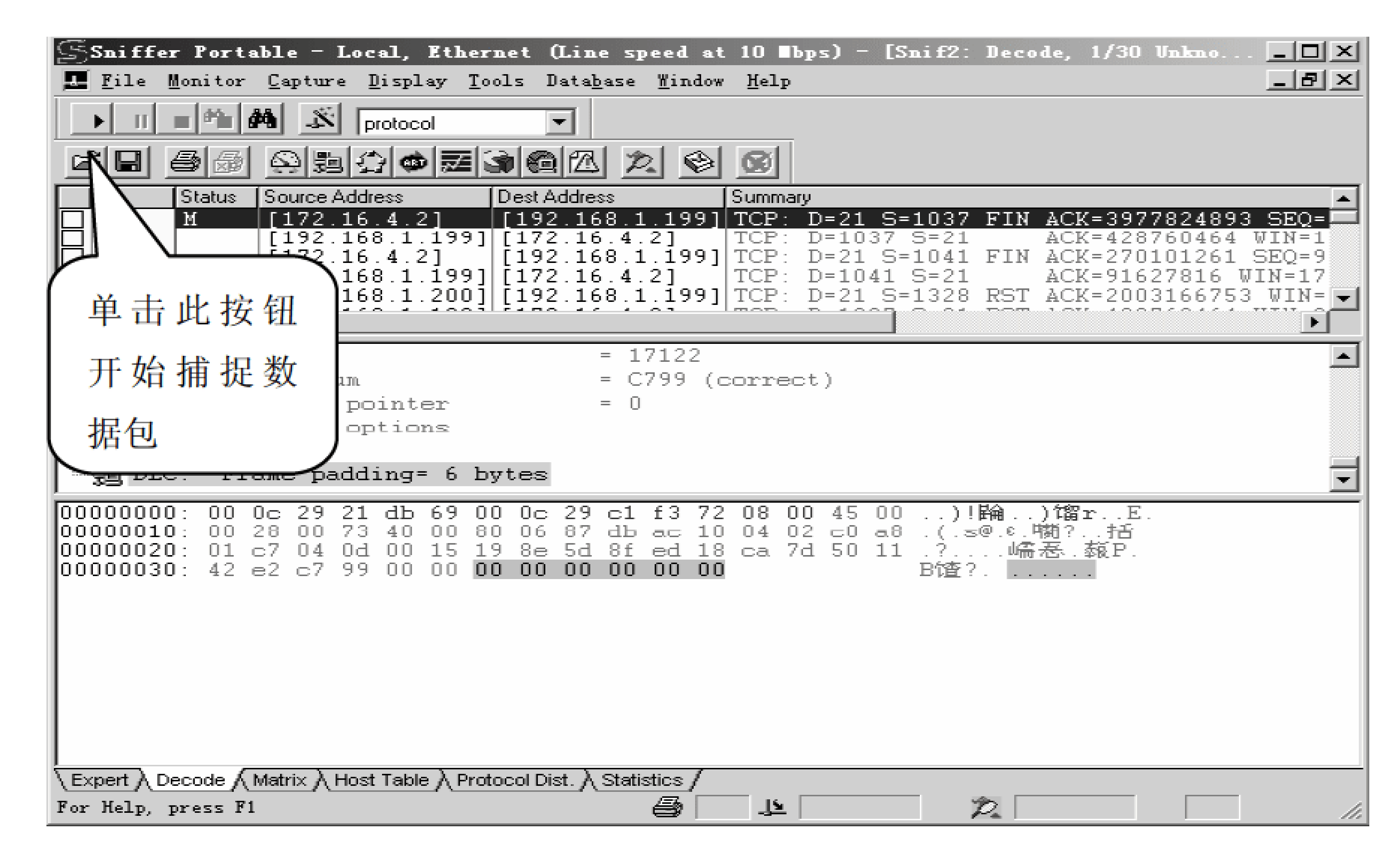


图 7-87

02 当 FTP 登陆过程捕捉完成后，单击工具栏上的【II】按钮，停止捕捉并显示捕捉到得数据包情况，如图 7-88 所示。

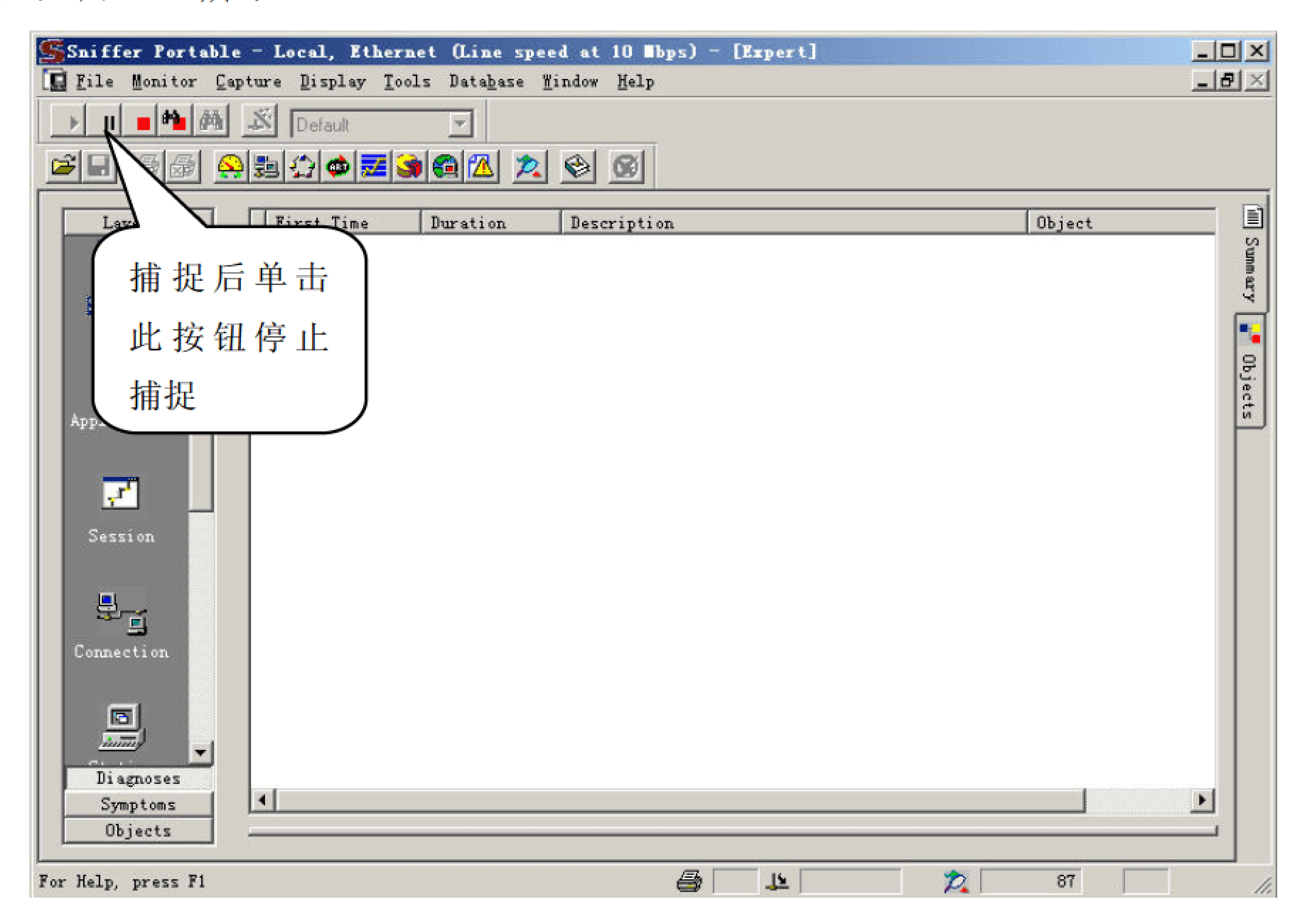


图 7-88

03 单击选中的【No】框中为“1”的那个数据包，进行分析。可以看到源 IP 为 172.16.4.2 的主机要访问目标 IP 为 192.168.1.199 的 FTP 服务，如图 7-89 所示。

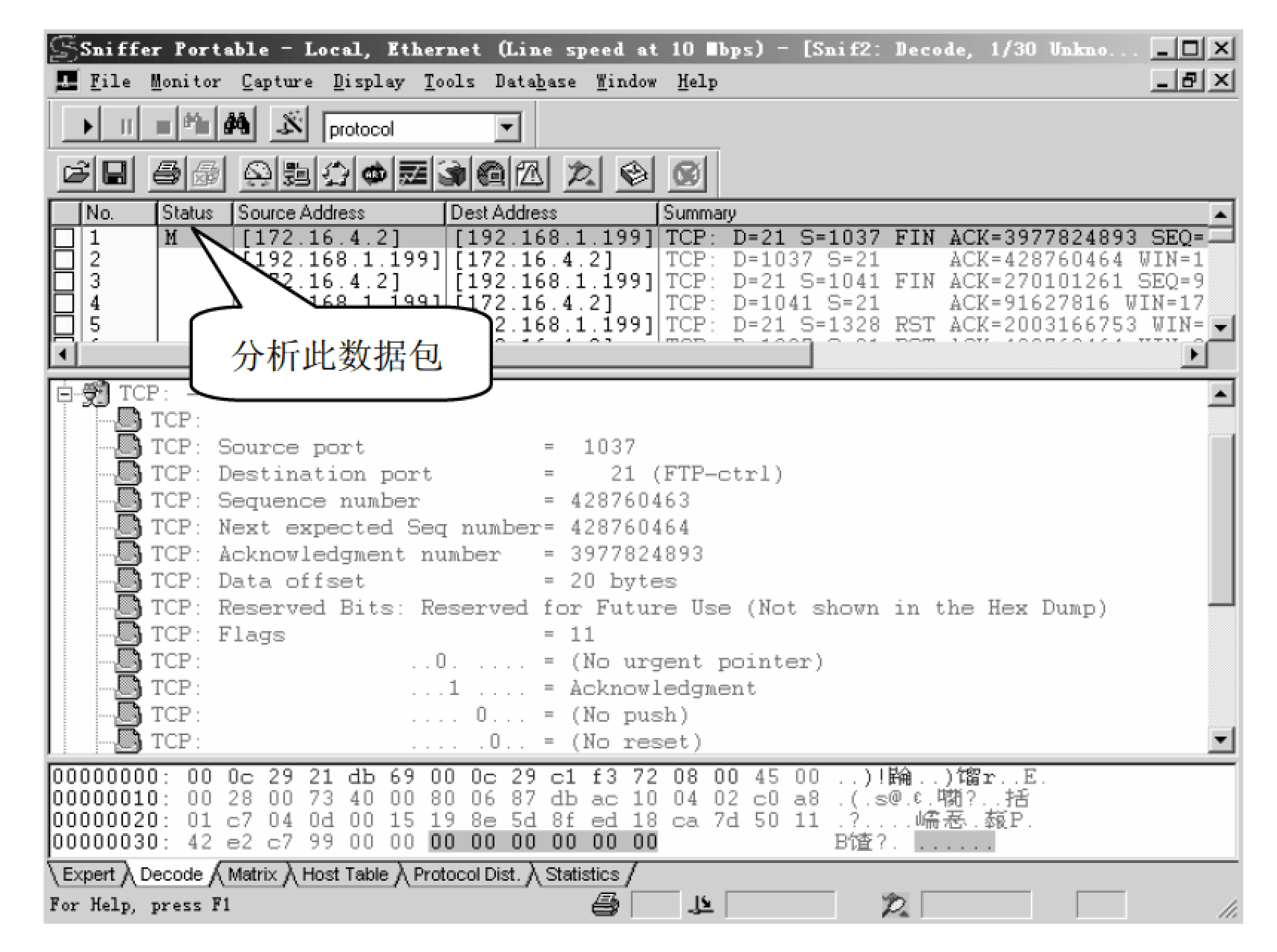


图 7-89



提示

通过图 7-89 可以看出该数据包在传输层使用的是 TCP 协议，其中【Source port】（源端口）是 1037，【Destination port】（目标端口）是 21，客户机访问目标主机的 FTP 服务。

04 从捕获到的数据中可以看出 FTP 在传输层使用的是 TCP 协议，在客户机登陆 FTP 成功之前首先需要进行 TCP 协议的三次握手，如图 7-90 所示。

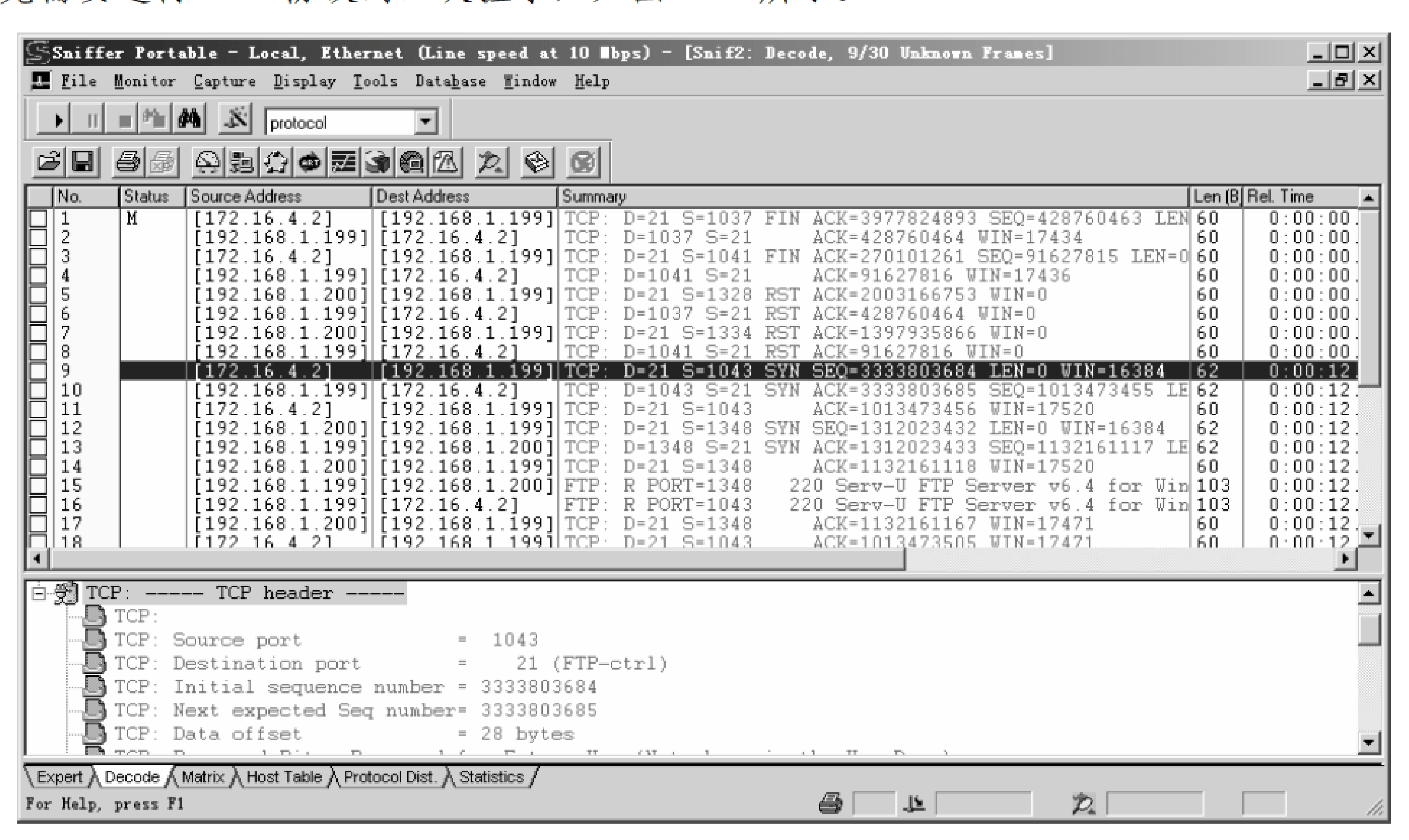


图 7-90

TCP 三次握手流程分析介绍如下。

- 观察图 7-90 中【No】框中“9”的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用目标端口 21，源端口 1043 向目标 IP 为 192.168.1.199 的目标主机发送 SYN 同步信息，这是第一次握手。
- 观察图 7-90 中【No】框中“10”的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用源端口 21，目标端口 1043 向目标 IP 为 172.16.4.2 的目标主机发送 SYN 同步信息和 ACK 确认信息，这是第二次握手。
- 观察图 7-90 中【No】框中“11”的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用目标端口 21，源端口 1043 向目标 IP 为 192.168.1.199 的目标主机发送 ACK 确认信息，这是第三次握手。

05 从捕获的数据中可以看出登陆 FTP 服务器需要对账户和密码进行验证，如图 7-91 所示。

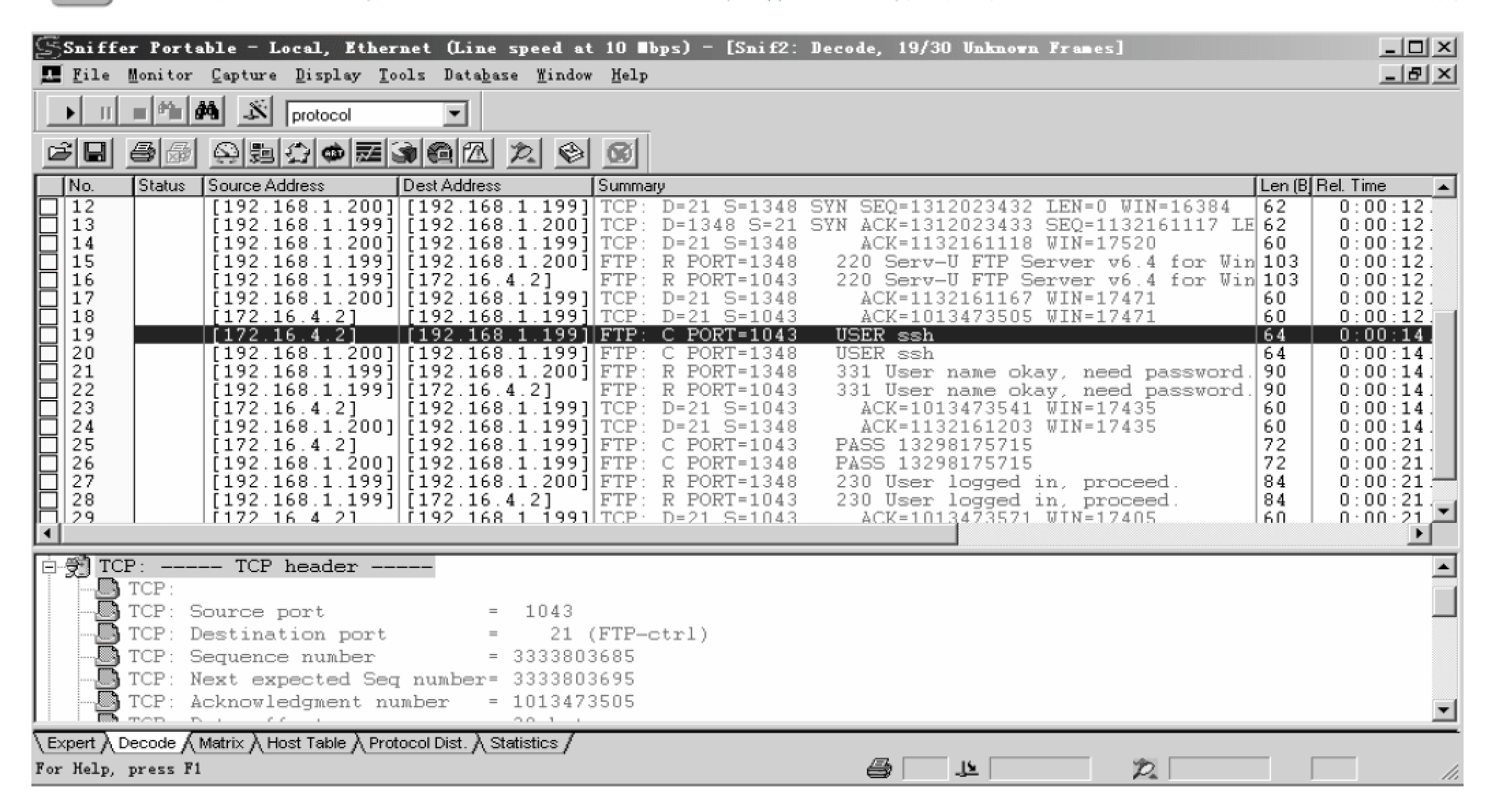


图 7-91

FTP 身份验证过程分析介绍如下。

- 观察图 7-91 中【No】框中“19”的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用端口 1043，向目标 IP 为 192.168.1.199 的目标主机发送“USER ssh”意为用户名为 ssh 的信息。
- 观察图 7-91 中【No】框中“22”的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用端口 1043，向目标 IP 为 172.16.4.2 的目标主机发送“User name okay，need password”意为用户名验证通过，需要密码信息。
- 观察图 7-91 中【No】框中“25”的数据包，可以看出源 IP 为 172.16.4.2 的源主机使用端口 1043，向目标 IP 为 192.168.1.199 的目标主机发送“PASS 13298175715”意为密码为 13298175715 的信息。
- 观察图 7-91 中【No】框中“28”的数据包，可以看出源 IP 为 192.168.1.199 的源主机使用端口 1043，向目标 IP 为 172.16.4.2 的目标主机发送“230 User logged in，proceed”意为用

户登陆成功的信息。

7.4.5 分析造成网络速度慢的原因

在日常的网络管理过程中，经常碰到的问题不是网络不通，而是网络的速度莫名其妙的变得很慢，但是找不到原因。这时可以借助 Sniffer Pro，通过对 Sniffer 的 HostTable 和 Matrix 进行分析可以轻松找到网络速度慢的原因。

具体操作步骤如下。

01 选择【Monitor】（监控）➢【HostTable】（主机列表）菜单命令，打开 Sniffer 的主机列表监控功能窗口，可以看到哪些主机在某段时间内传输的数据特别多，如图 7-92 所示。

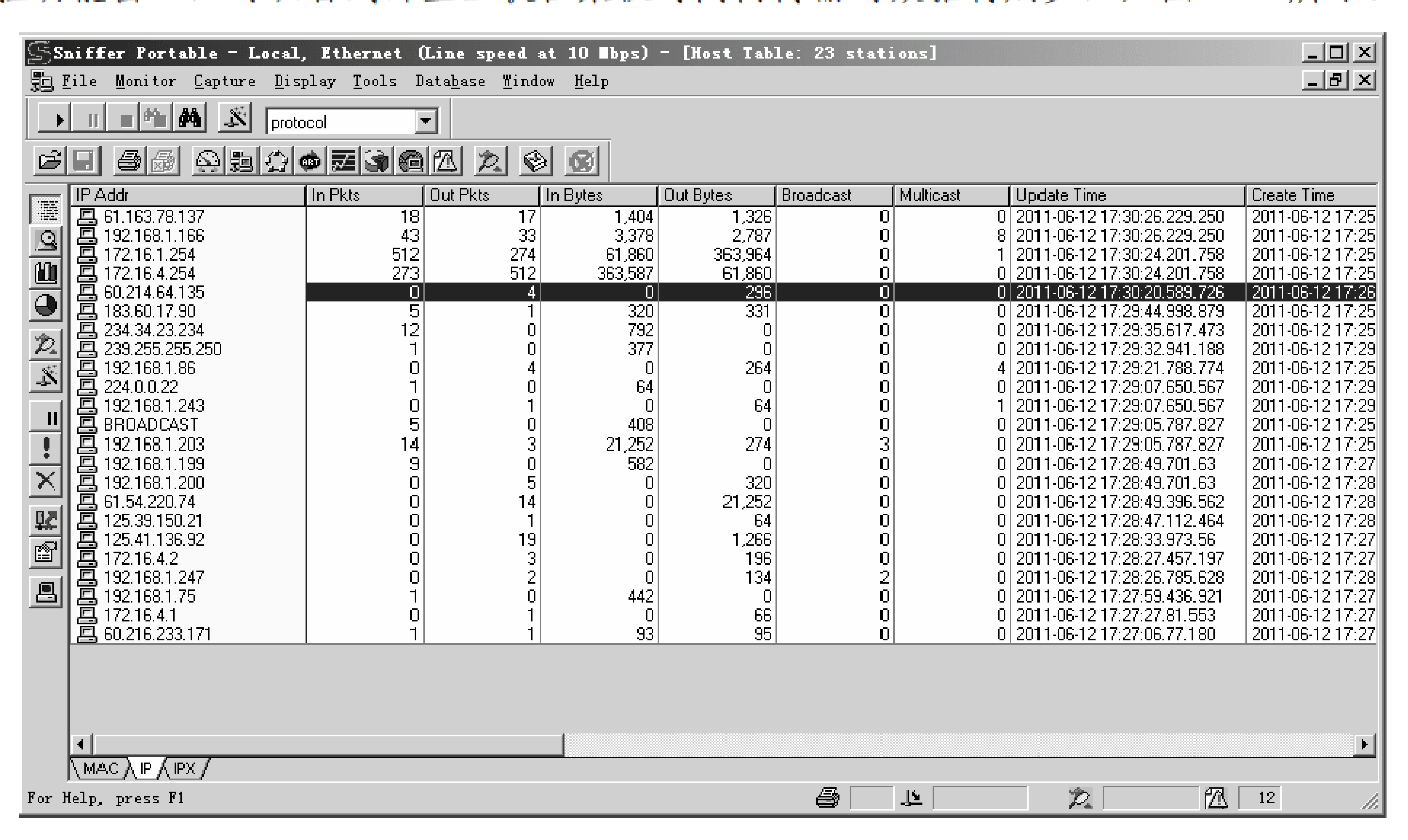


图 7-92

02 选择【Monitor】（监控）➢【Matrix】（矩阵）菜单命令，打开 Sniffer 的矩阵监控功能。通过【Matrix】矩阵监控功能查看数据传输特别多的那些主机都在和什么主机通信，如图 7-93 所示。如果发现这些主机在某些特定的时段传输数据量特别大并且是和大量的不同主机进行并发连接，这时候就可以怀疑是这些主机在进行 p2p、BT 下载或者是中蠕虫病毒，导致网络效率底下，影响到了网速。

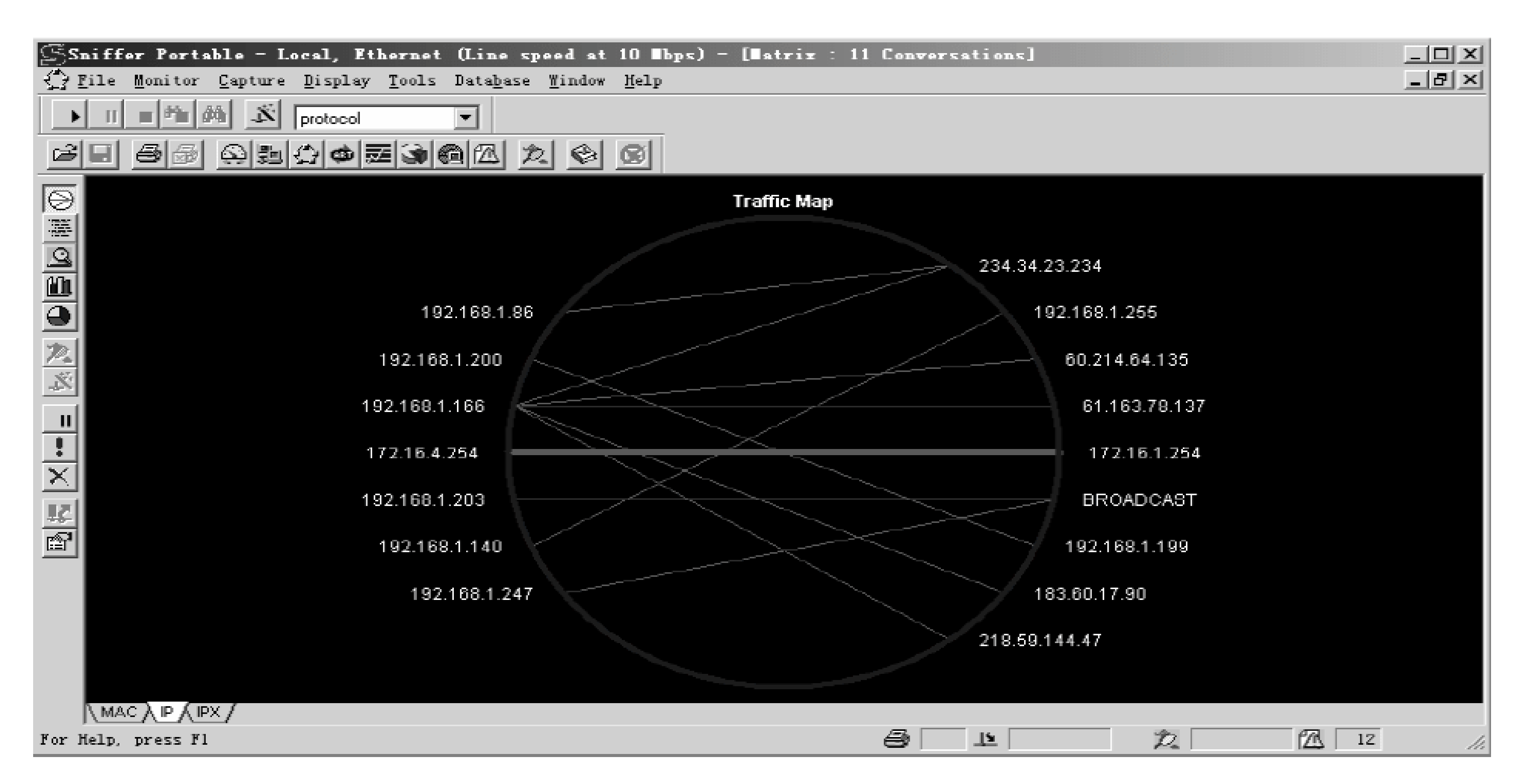


图 7-93

7.4.6　查找网络 ARP 攻击源

在局域网通信的过程中，当源主机在请求 ARP 解析的时候，ARP 攻击者伪装目的主机的 MAC 地址返回给源主机，这时源主机就会对接收到的错误目标 MAC 地址进行访问，使得网络内部出现大量的无用广播流量影响网络效率，这就是 ARP 攻击或者是 ARP 欺骗。

通过 Sniffer Pro 查找网络 ARP 攻击源的具体操作步骤如下。

01 在 Sniffer Pro 的操作界面单击菜单【Capture】（捕捉）➢【Define Filer】（定义过滤器）菜单命令，弹出【Define Filter – Capture】（定义捕捉过滤器）对话框，单击【Profiles】（配置文件）按钮，如图 7-94 所示。

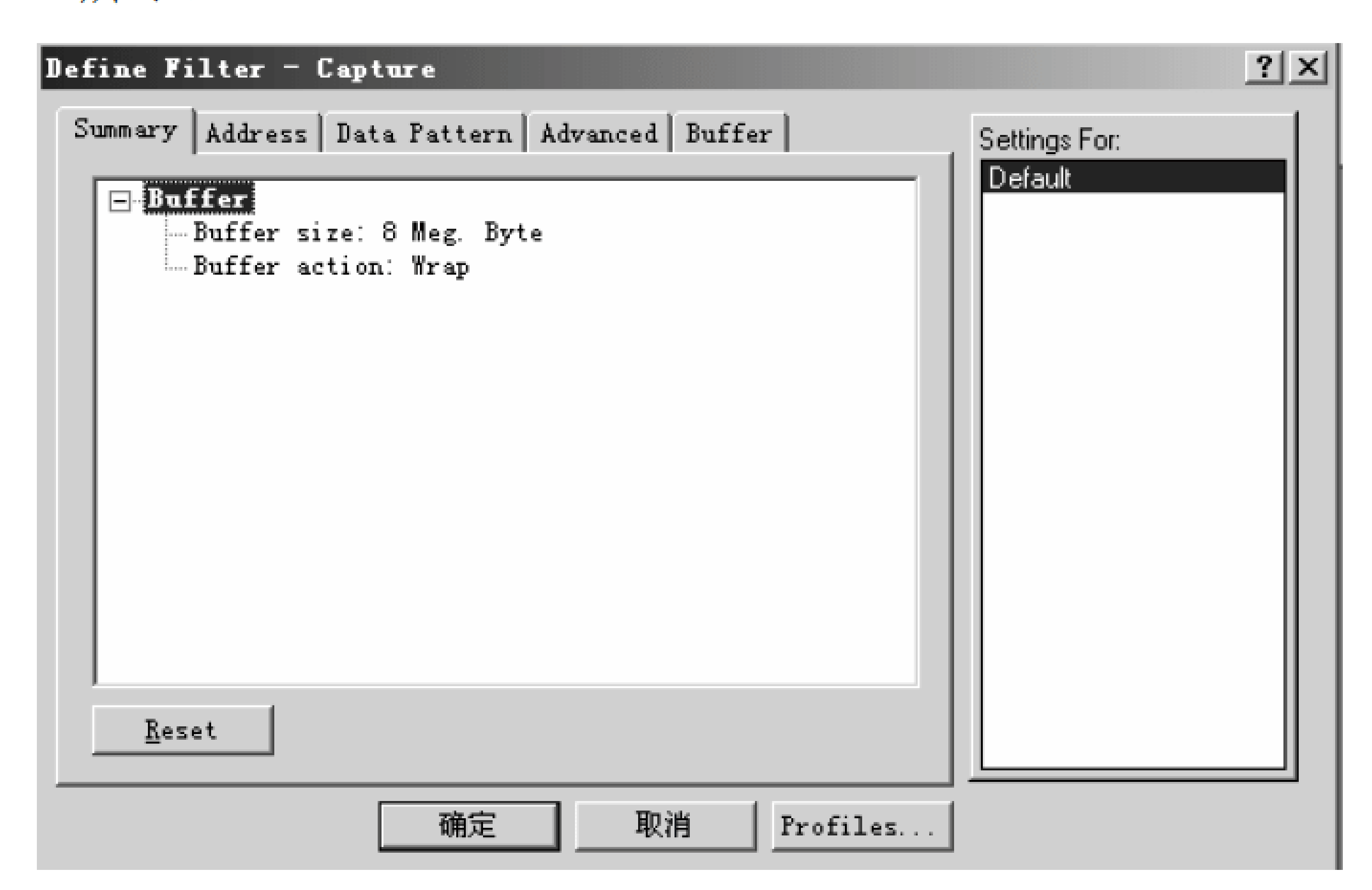


图 7-94

02 弹出【Capture Profiles】（捕捉配置文件）对话框，单击【New】(新建)按钮，如图 7-95 所示。

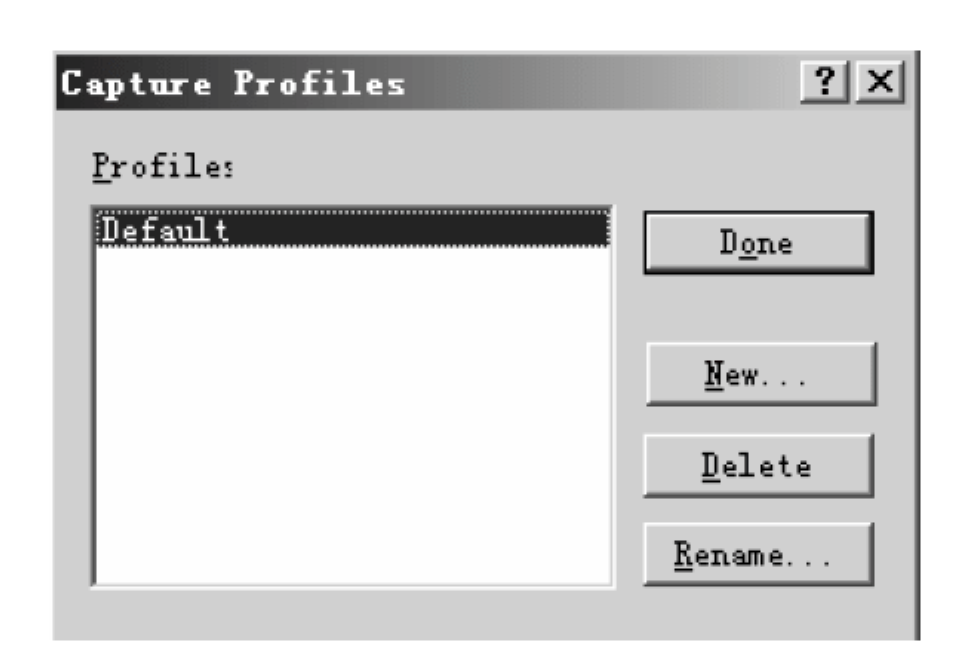


图 7-95

03 弹出【New Capture Profile】（新的捕捉配置文件）对话框，在【New Profile Name】（新的配置文件名字）文本框输入过滤器的名字“ARP”，单击【OK】（确定）按钮，一个新的过滤器创建完成，如图 7-96 所示。

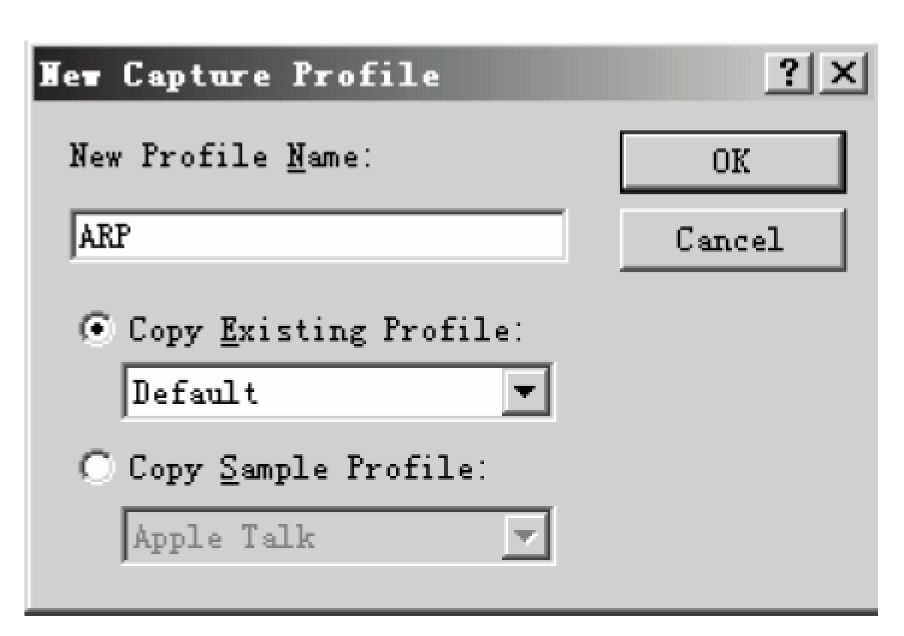


图 7-96

04 返回【Capture Profiles】（捕捉配置文件）对话框，单击【Done】（是）按钮，如图 7-97 所示。

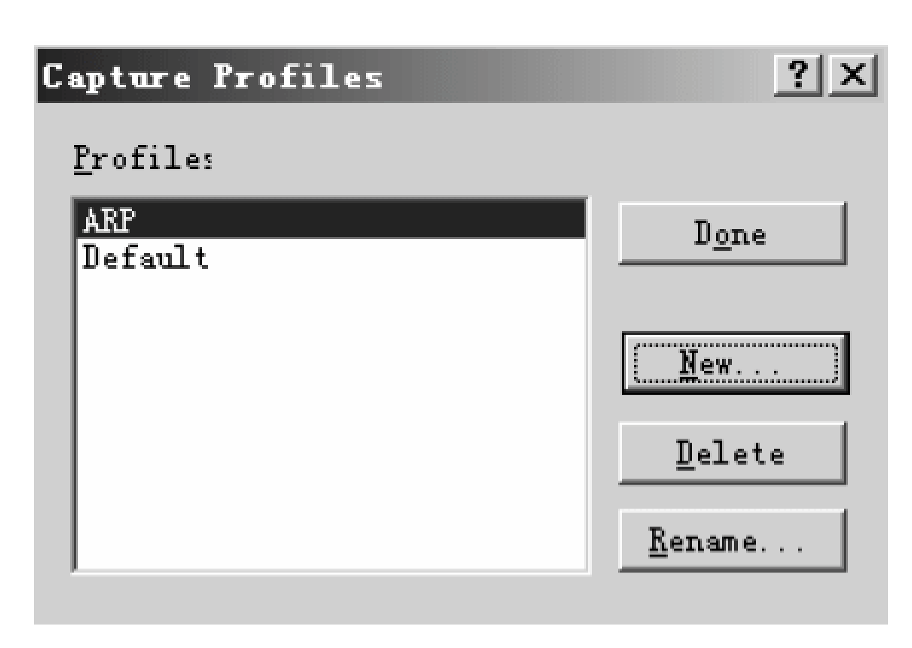


图 7-97

05 返回【Define Filter – Capture】（自定义捕捉过滤器）对话框，选择【Advanced】（高级的）选项卡，选中【IP ARP】协议，一个新的 ARP 协议过滤器创建完成，如图 7-98 所示。

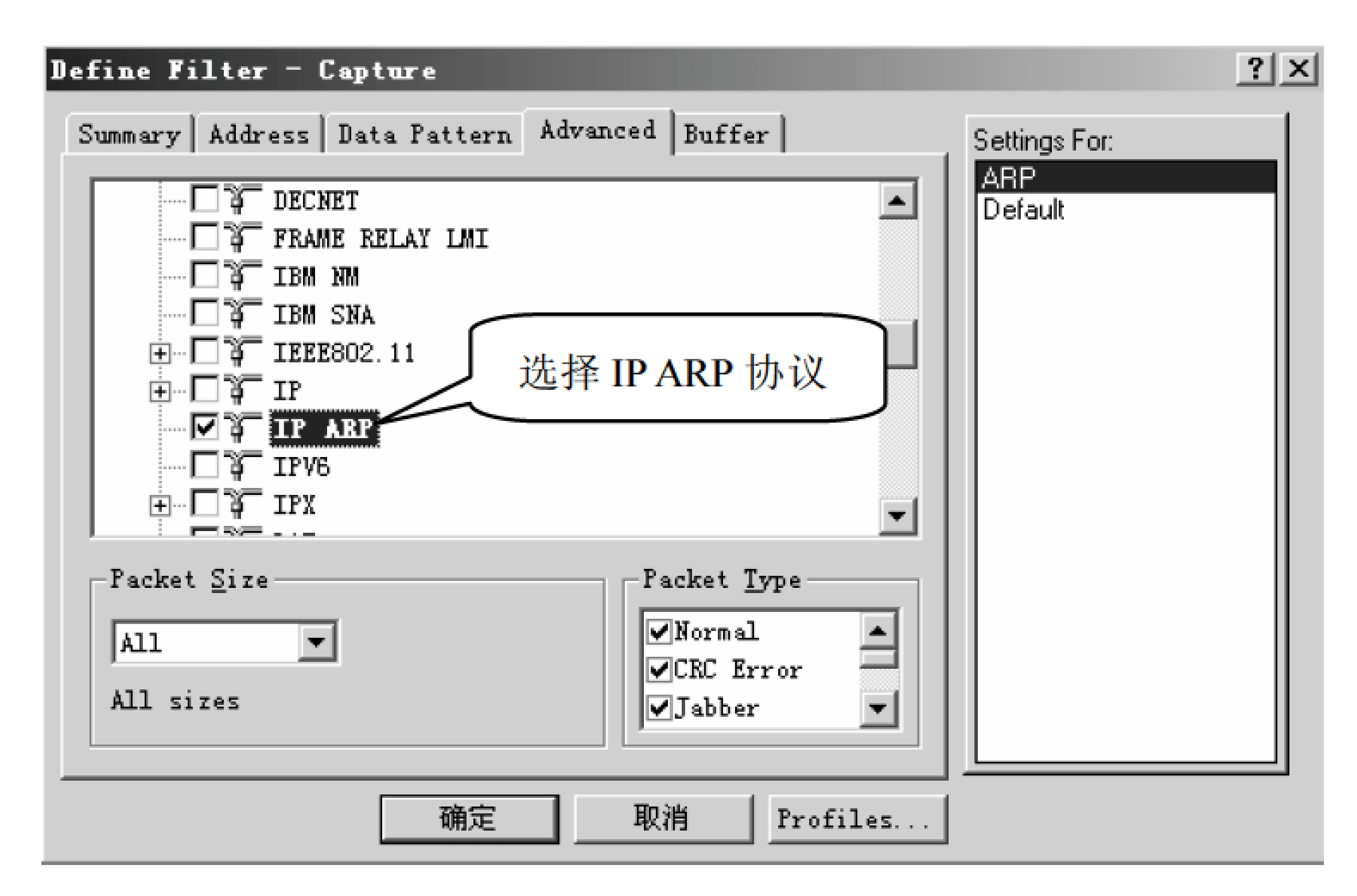


图 7-98

06 单击工具栏上的【▶】按钮，开始捕捉数据包，如图 7-99 所示。

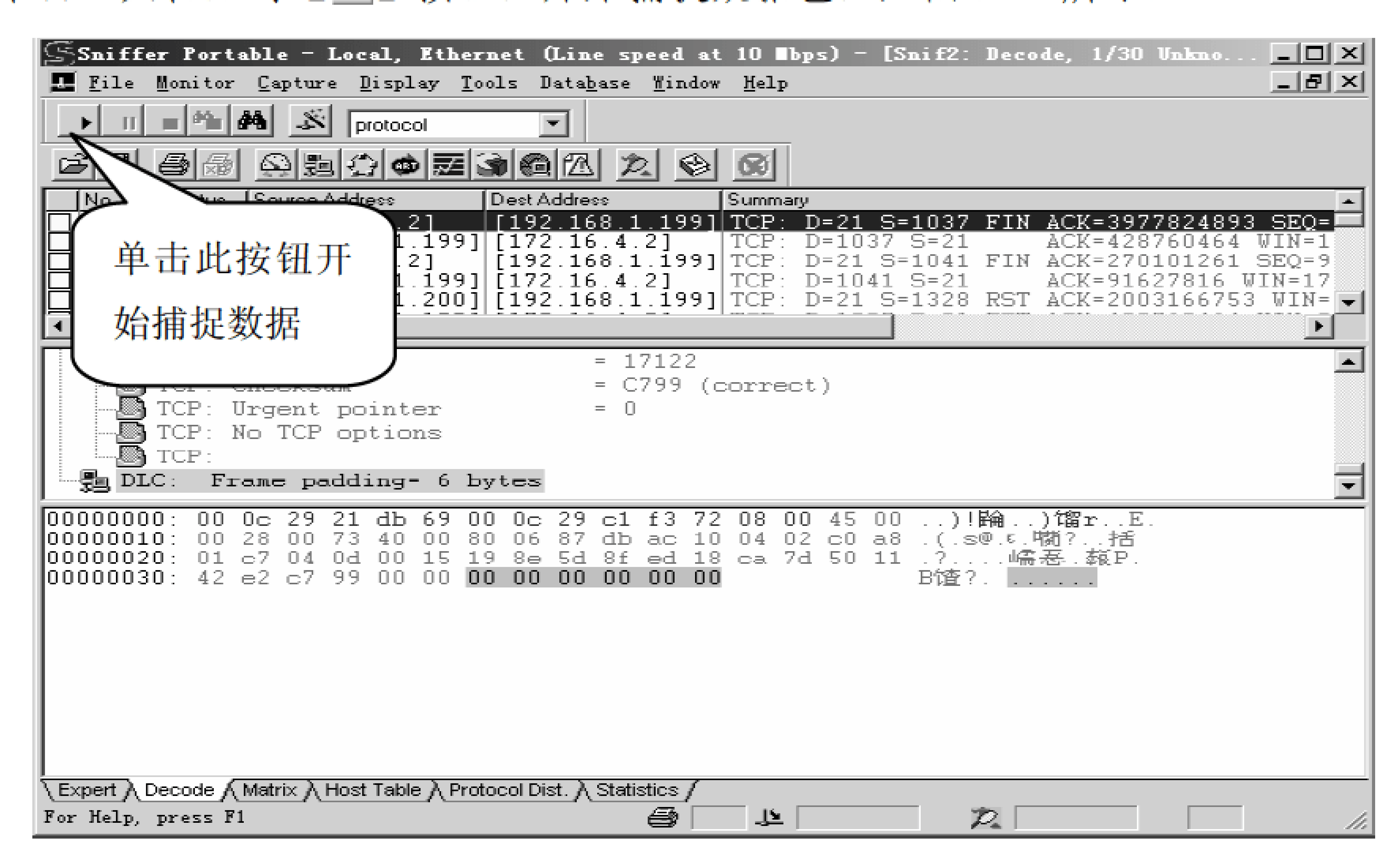


图 7-99

07 过一段时间后单击工具栏上的按钮【Ⅱ】，停止捕捉并显示捕捉到的数据包情况，如图 7-100 所示。

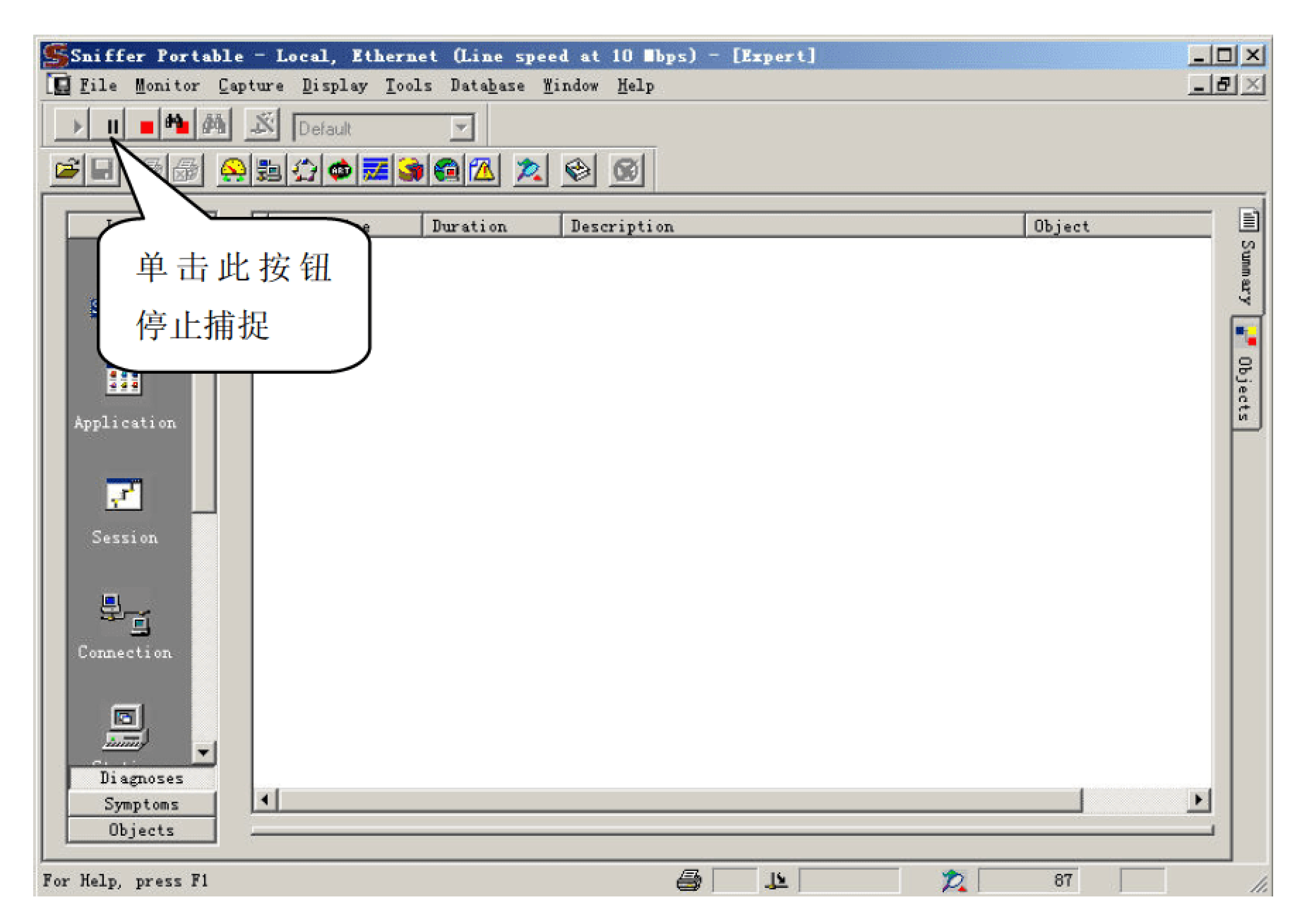


图 7-100

08 选择【Monitor】（监控）➢【Matrix】（矩阵）菜单命令，打开 Sniffer 的矩阵监控功能，如图 7-101 所示。

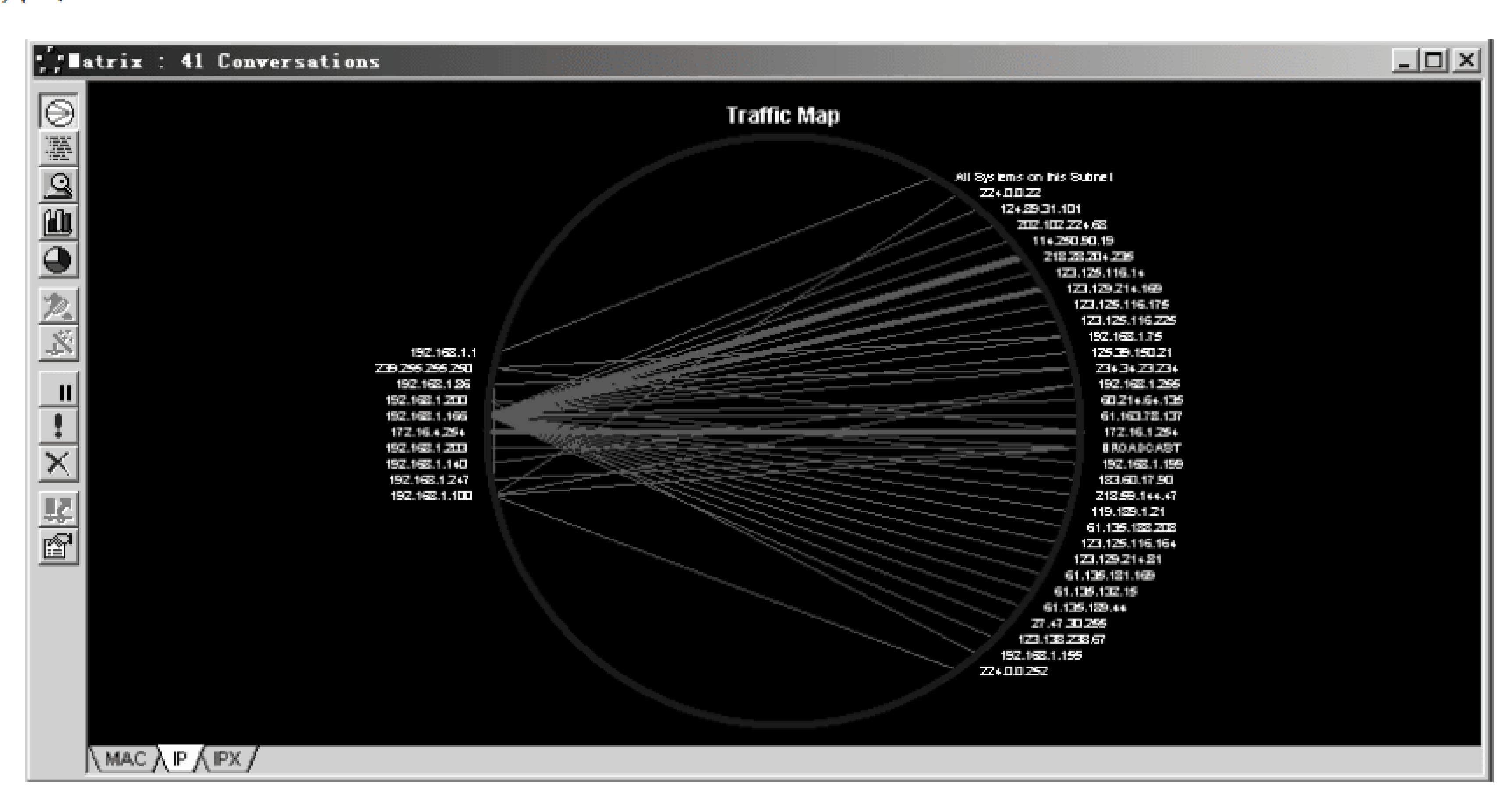


图 7-101



观察图 7-101 中的数据通信，如果发现有某一个主机正在和局域网内大量的主机进行并发连接，那么就可以怀疑该主机中了 ARP 病毒或者是人为在进行 ARP 攻击，网络管理员应该及时找到该主机并采取相应措施。

09 在复杂的网络环境中，如果要单独查看某个主机的通信情况，比如查看 IP 为 192.168.1.199 的主机通信情况，右击“192.168.1.199”，在弹出的快捷菜单中选择【Show Select Node】（显示选择的节点）菜单命令，如图 7-102 所示。

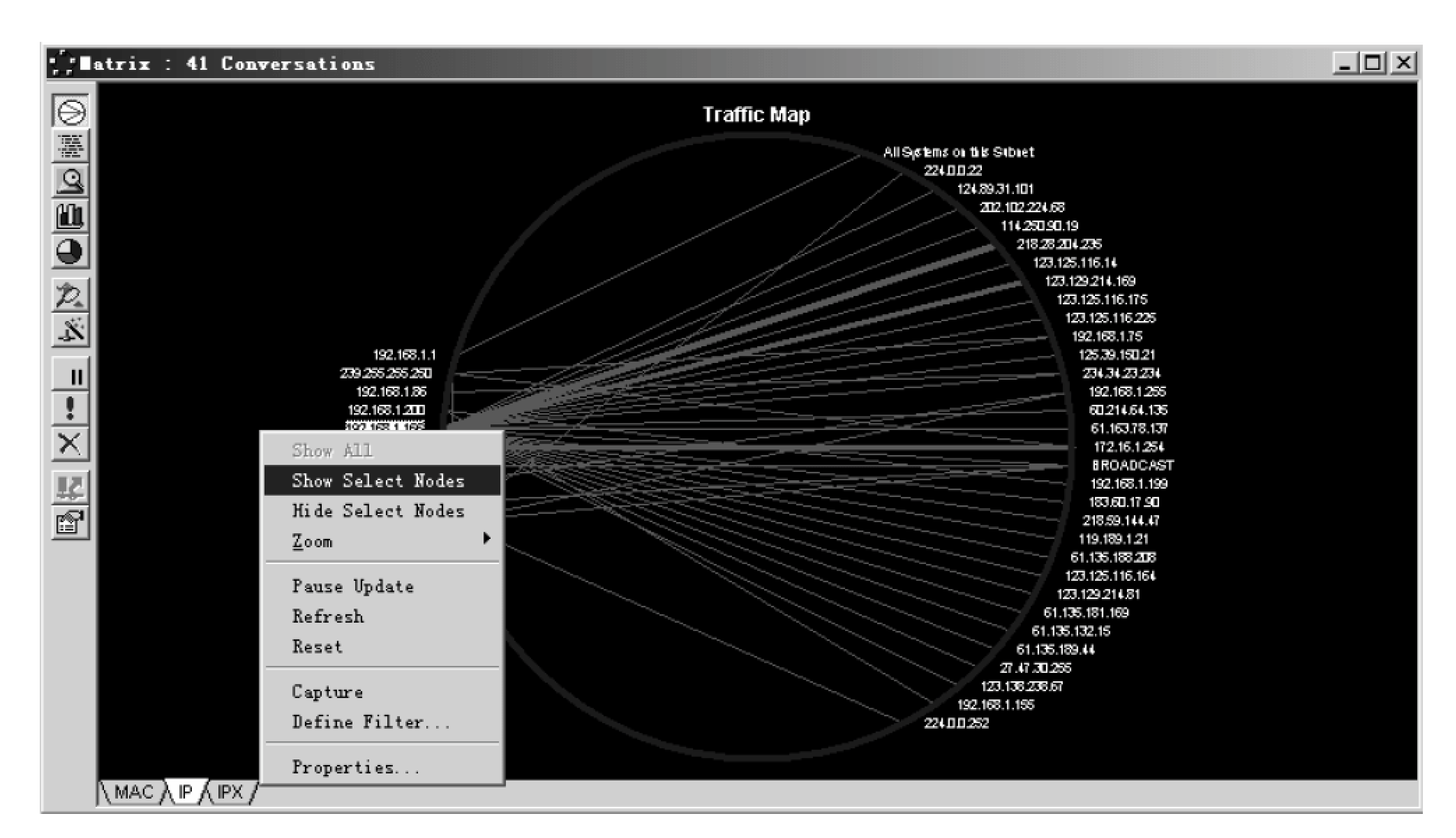


图 7-102

10 弹出 IP 为“192.168.1.199”的主机的通信情况的矩阵信息，如图 7-103 所示。

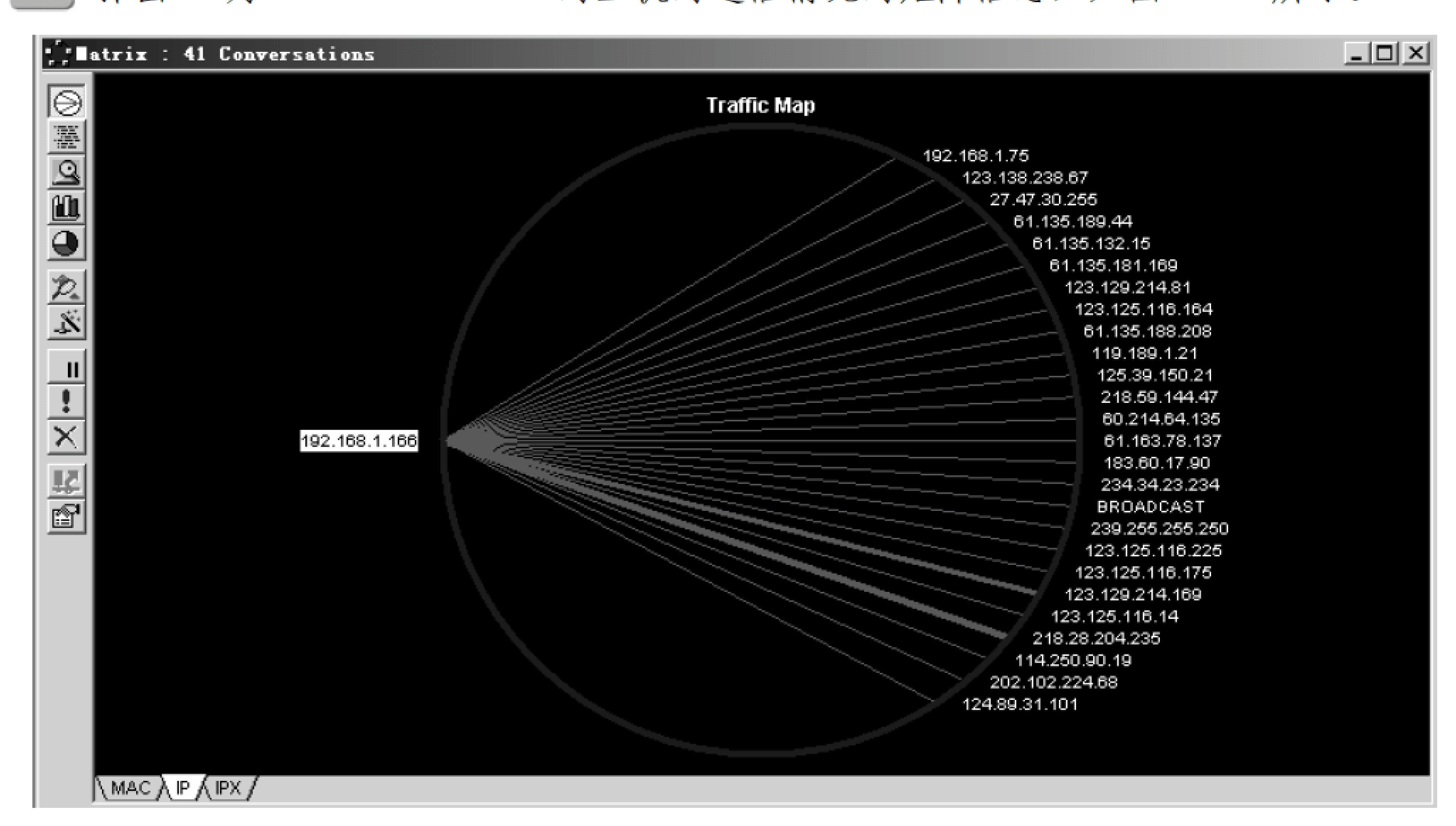


图 7-103



提　示

如果该主机正在和大量的外网主机并发通信并有大量的数据包传输出现，就有可能是该主机正在进行 P2P、BT 等下载，如果该主机正在和大量内网主机并发通信，则有可能中了 ARP 病毒、蠕虫、或者是人为的安装了 P2P 攻击软件，并且正在进行 ARP 攻击，这时网络管理员就可以根据 IP 或者 MAC 地址找到该主机，然后采取相应措施。

7.5 专家答疑

（1）安装 Sniffer Pro 软件，打开软件包后，软件的界面显示不完整，或者有时候会显示网页显示不完整，应该怎么解决？

答：Sniffer Pro 的界面显示需要 Java 的 JDK 支持，安装 JDK 即可。有的时候安装完 JDK 再打开 Sniffer Pro 后，也会出现网页错误的提示，这是因为计算机的 IE 版本过低，升级 IE 版本即可。

（2）安装完 Sniffer Pro 后进行数据包捕捉，可是在菜单栏【Capture】（捕捉）菜单中，【Stop and Display】（停止并显示）选项却是灰色的，使得无法停止数据包的捕捉？

答：关于捕捉数据包后无法停止数据包捕捉的问题，一般是因为 Sniffer Pro 没有正常捕捉到数据包，这时候就需要考虑 Sniffer Pro 的安装位置是否合适，或者 Sniffer Pro 监听网卡是否没有监听到数据包。

第 8 章　企业网络监控系统

随着企业信息化的发展，企业的办公越来越依赖网络，一个高效的网络就成为企业办公的必要保障。并且随着企业信息化建设的不断发展，各种网络应用、网络流量以及员工规模都在不停的增长，企业网络带宽往往由于分配不合理，或者员工的上网行为得不到很好的管理控制，导致企业重点应用出现访问迟缓甚至无法访问的情况，这时候就需要一个高效的网络监管分析工具，时刻对员工的上网行为和网络带宽分配进行监测，合理的分配带宽使用，提高网络利用效率。

8.1　网络监管系统的意义

随着信息化在企业中的普及，各个公司对网络的要求也越来越高，网络运行的良好与否已经成为公司效率高低的一个衡量标准。但是在网络出现故障的很多时候，网络管理员不知道该从什么地方查找故障，在平时也找不到好的方法预防故障。这时候就需要用到网络监管分析，合理的限制和分配网络资源，对所有用户的上网行为进行严格监控并记录在案，以备日后查询。

同时，公司的各种内部机密信息也有可能被员工无意中通过邮件或者 FTP 等方式发送给外部人士，这给公司的信息机密带来很大威胁，而网络监管可以进行关键字过滤，防止公司信息在网络中进行传输。

公司的信息监管需要和网络管理需求都促使了网络监管工具的产生，合理的使用网络监管分析工具可以有效的提高公司办公效率和网络运行效率。

8.2　主流监控产品

要进行网络监管分析，就需要具备有利的监控产品。下面介绍市场上主流的监控产品 Red Eagle 和网路岗。

8.2.1　网络监管专家—Red Eagle

网络监管专家—Red Eagle 是专门针对企业网络管理开发的，是公司管理和公司网络管理中不可缺少的一个好工具。网络监管专家可以帮助网络管理员全面的掌握员工上网行为，根据员工角色的不同严格规范员工的上网行为，同时能够根据公司的需要引导员工更合理的利用工作时间，通过

对各种网络资源下载和对各种娱乐网站、娱乐视频的限制，大大提高了工作效率。

另外针对公司内部机密信息，网络监管专家可以对员工的邮件，通信记录进行关键字过滤，时刻保护公司内部私密资料的安全，并且通过日志的归类和记录，提供追查私密资料泄露的依据，确保各种网络资源被合理、高效的使用。

同时，该软件还提供了各种局域网内协同工作的便利机制。它广泛适用于各种政府机构、企事业单位、工厂、医院、网吧、学校等的内部网络，可以非常方便的完成集中监控管理任务。

8.2.2 网路岗七代网络监管工具

网路岗七代作为一款行业领先的局域网管理监控软件产品，在国内同类软件产品中市场占有率达到第一，并且经过多年的更新升级，目前网路岗最高版本为第七代。和旧的版本相比，最新版本的网路岗网络监管工具不仅性能齐全，其稳定友好的操作界面也深受网络管理人员的喜爱。下面简要介绍网路岗七代网络监管工具的主要功能。图 8-1 为网路岗七代的主操作界面。



图 8-1

网路岗七代的主要功能包括如下。

（1）QQ/MSN 聊天内容全纪录(不需要安装客户端)，限制登录指定的 QQ 号，MSN 账号；

（2）记录/封堵 BBS/申请服务/发表文章(外发尺寸限制)、博客/空间发表文章等；

（3）邮件监控功能，监控网页发送邮件内容及附件和客户端(包括 smtp/pop3)收发的邮件；

（4）提供全面的过滤规则，对相关的网站进行过滤及封堵原因记录；

（5）敏感行为的实时报警(声音报警/邮件报警/GSM 报警)；

（6）封堵常用网络软件(QQ/BT/电驴/MSN 等等)；

（7）支持网桥，NAT 代理上网监控；

（8）FTP 上传文件的记录；

（9）通过安装插件还可以控制电脑的 USB 存储，截取电脑的屏幕，监控电脑里的文件；

（10）网络流量监控，可监控局域网内电脑的时流量，包括上行流量和下行流量的大小；

（11）自动实时员工上网评价，自定义不规范上网行为；

（12）网路岗新增局域网限速功能，可以有效控制局域网内电脑文件的上传，下载速度。

8.3 项目实施：使用网路岗进行网络监管

网路岗七代网络监管工具是一款非常成熟的网络监管分析软件，通过软件的部署，可以轻松对企业内部的计算机的上网行为进行严格监管，提高网络运行效率。对员工对外通信进行关键字过滤，保护了内部私密信息，同时网路岗七代日志对员工上网行为进行归档和记录，为日后出现网络故障和信息泄密情况提供分析依据。

和网路岗六代相比，网路岗七代又增加了很多新的功能，下面将针对网路岗七代的主要功能做讲解。

8.3.1 安装和注册网路岗七代

1. 选择网路岗七代安装的位置

如果要利用网路岗对用户进行流量限制，网路岗的安装位置则特别重要，因为安装位置决定了是否能够充分发挥网路岗的功能。网路岗的安装位置一般有以下两种选择。

（1）网路岗配置双网卡网桥模式。

（2）网路岗安装在代理服务器上进行带宽控制，网络限速。比如安装在 ISA 服务器、Windows Server 2003 代理服务器上等。

在本章的实例中，网路岗七代软件安装位置采用第二种，如图 8-2 所示。

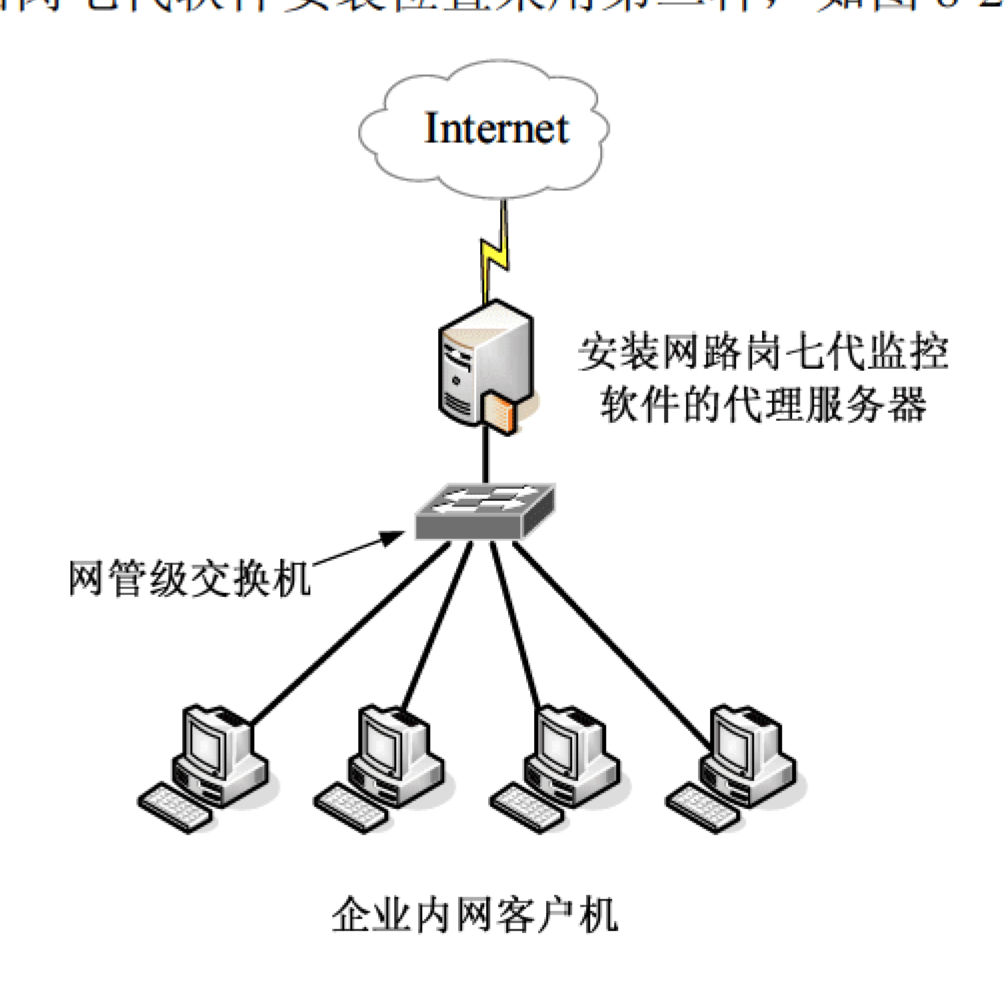


图 8-2

2. 安装网路岗七代网络监管软件

网路岗七代监控软件分为服务器端软件和客户端软件，一般情况下只需要在服务器端安装服

务器软件，在安装的时候注意正确选择。

安装网路岗七代监管软件的具体操作步骤如下。

01 双击网路岗七代监管软件的服务器端安装文件，在弹出的【网路岗.第七代】安装对话框中，单击【下一步】按钮，如图 8-3 所示。



图 8-3

02 弹出【许可证协议】对话框，选择【我接受该许可协议中的条款】单选按钮，表示同意网路岗第七代的安装许可协议，单击【下一步】按钮，如图 8-4 所示。

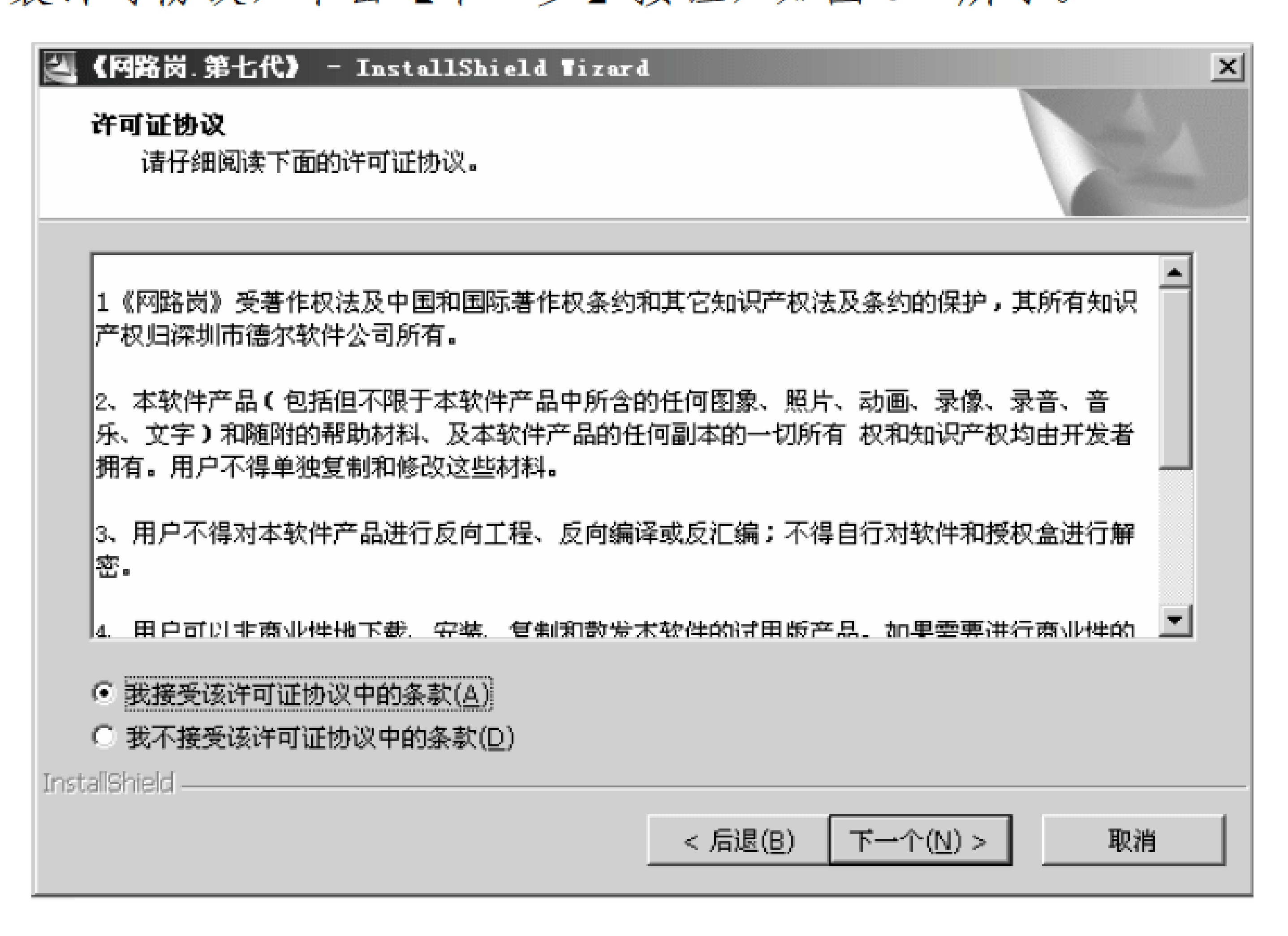


图 8-4

03 弹出【保存文件的位置】对话框，单击【更改】按钮，自定义网路岗七代网络监管软件的安装路径，本实例中采用默认安装路径“C:\Program Files\softbar.com\Sentry7”，单击【下一步】按钮，如图 8-5 所示。



图 8-5

04 网路岗第七代网络监管软件安装正在继续，并显示安装进度，如图 8-6 所示。



图 8-6

05 正在安装网路岗第七代的各种服务，等待安装服务界面消失，就意味着网路岗七代监管软件安装结束，如图 8-7 所示。

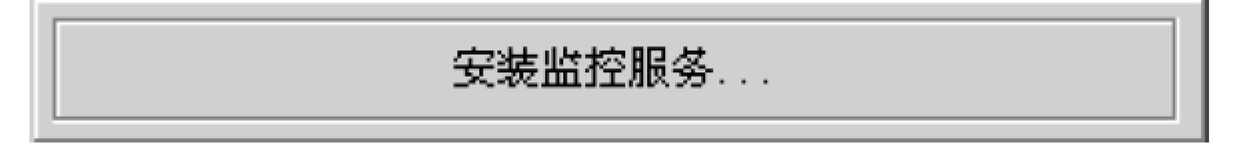


图 8-7

06 双击桌面上的【网路岗 7】快捷方式，打开网路岗的操作界面，单击【产品信息】按钮，如图 8-8 所示。



图 8-8

07 弹出【关于网路岗】对话框，单击【注册】按钮，如图 8-9 所示。



图 8-9

08 弹出【注册产品】对话框，在【序列号】、【公司名称】、【联系人】、【联系邮箱】和【联系电话】对话框中分别输入相关信息，然后单击【注册】按钮，如图 8-10 所示。



图 8-10

09 弹出【注册产品】提示框，单击【确定】按钮，如图 8-11 所示。



图 8-11

10 返回至【关于网路岗】对话框，单击【确定】按钮，表示网路岗七代网络监管软件安装注册完成，如图 8-12 所示。



图 8-12

8.3.2 设置网络监控模式

设置合理的网路岗监控模式有助于更好的监控网络内部计算机的数据流，设置网络监控模式的具体操作命令如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代监控软件的操作界面，单击【网卡/模式】下拉菜单，勾选内网网卡复选框，表面检测流经内网网卡的所有数据流，本案例中选择 IP 地址为 172.16.4.254 的网卡，如图 8-13 所示。

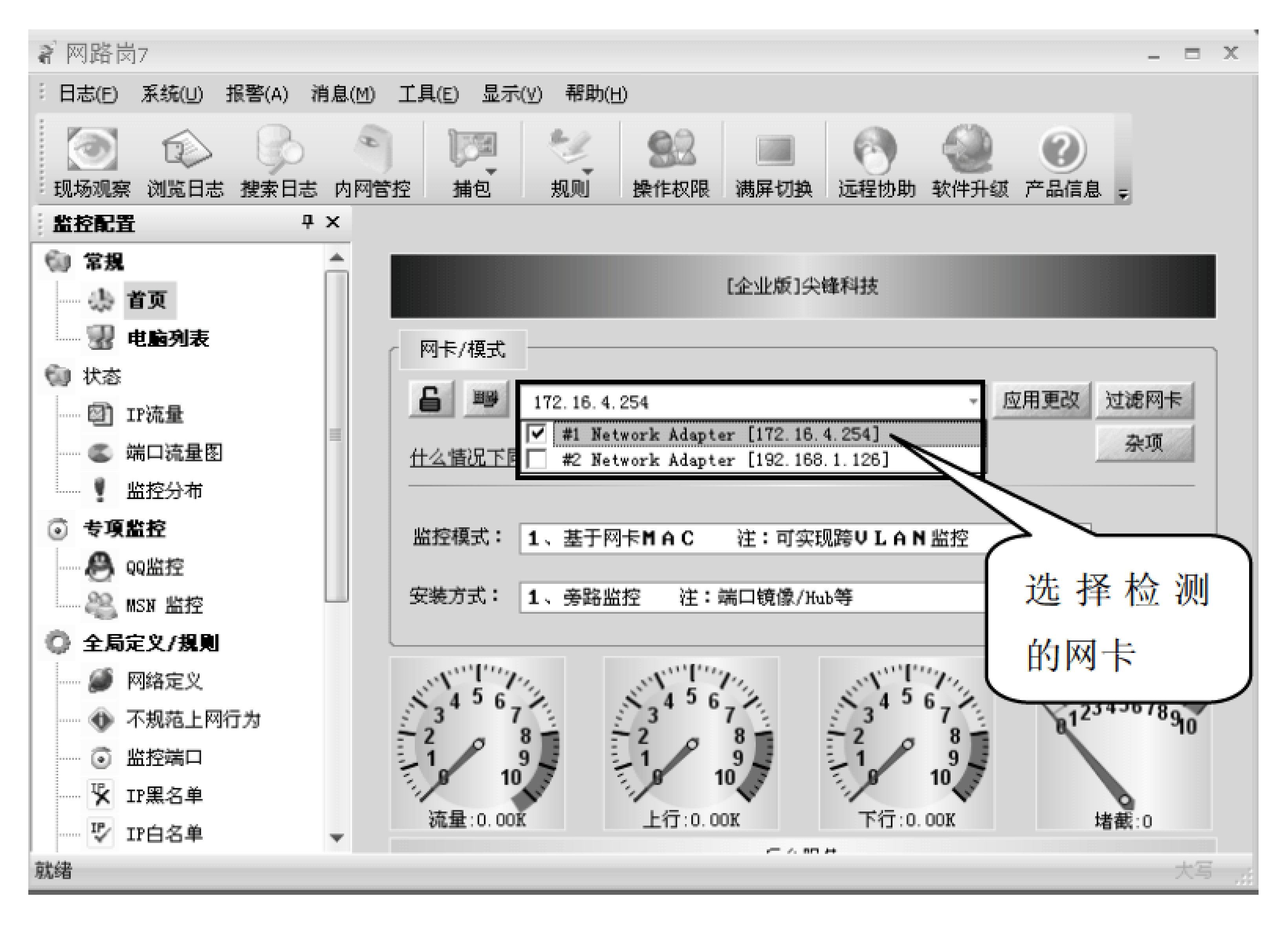


图 8-13

02 单击【监控模式】下拉菜单，在弹出的下拉菜单中选择【3、基于 IP】选项，如图 8-14 所示。

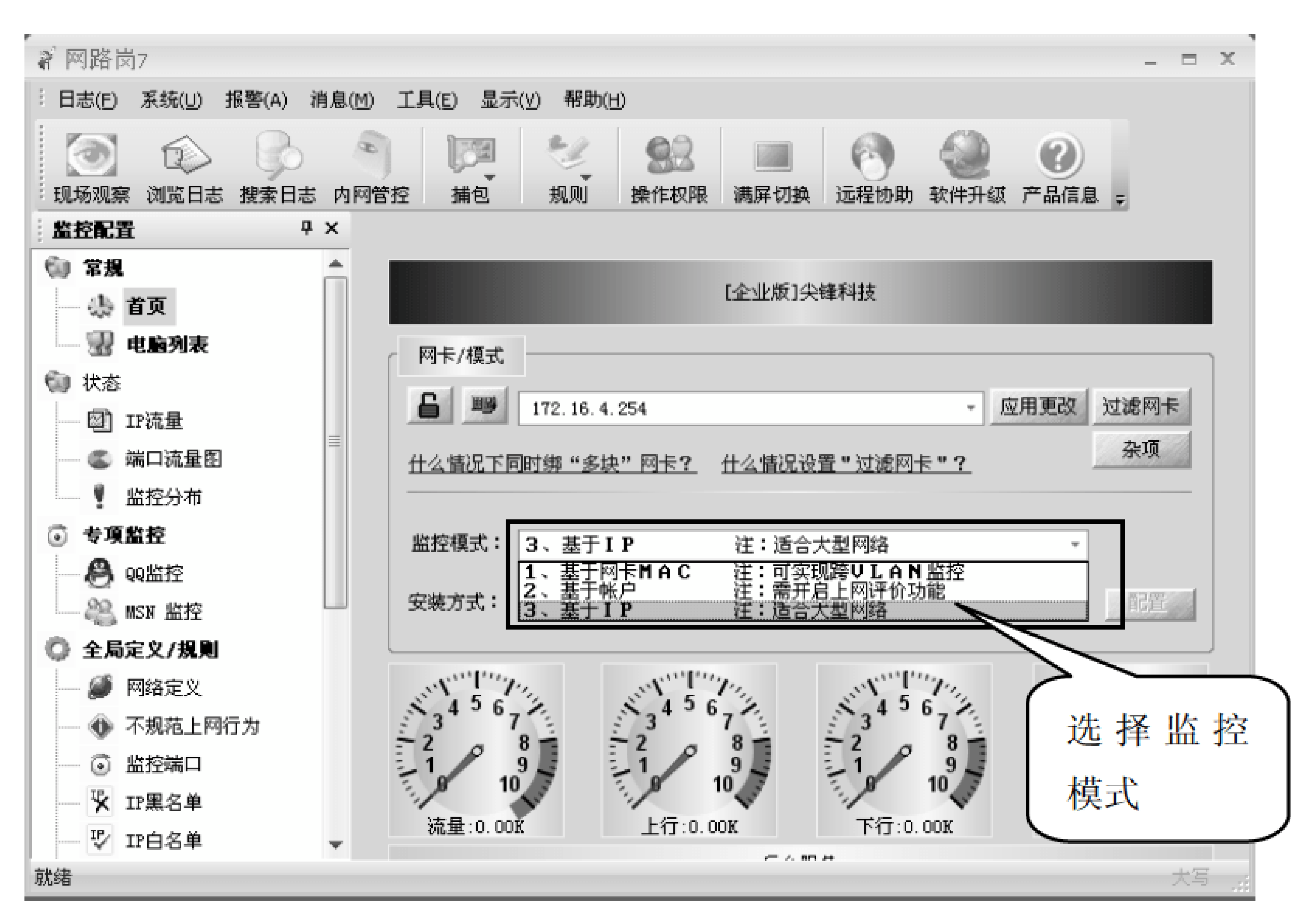


图 8-14

03 单击【安装方式】下拉菜单，在弹出的下拉菜单中选择【2、挂靠方式】选项，单击【应用更改】按钮，如图 8-15 所示。



图 8-15

04 弹出【绑定网卡】提示框，单击【继续】按钮，如图 8-16 所示。



图 8-16

05 返回至网路岗操作界面，单击【全部启动】按钮，启动网路岗七代的服务，完成网路岗七代网络监管工具的网络监控模式设置，如图 8-17 所示。



图 8-17

8.3.3 监管内部计算机并设置监控状态

网路岗七代监管软件的主要功能就是对内部网络计算机的上网行为进行管理，有了网路岗七代监管软件，网络管理员可以很轻松的了解网络内部每个计算机的网络使用情况，但前提是网路岗七代监管软件监管这些计算机。

使用网路岗七代监管软件监控网络内部的计算机的具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代监管软件的操作界面，单击左侧【电脑列表】选项，单击【扫描】按钮，如图 8-18 所示。

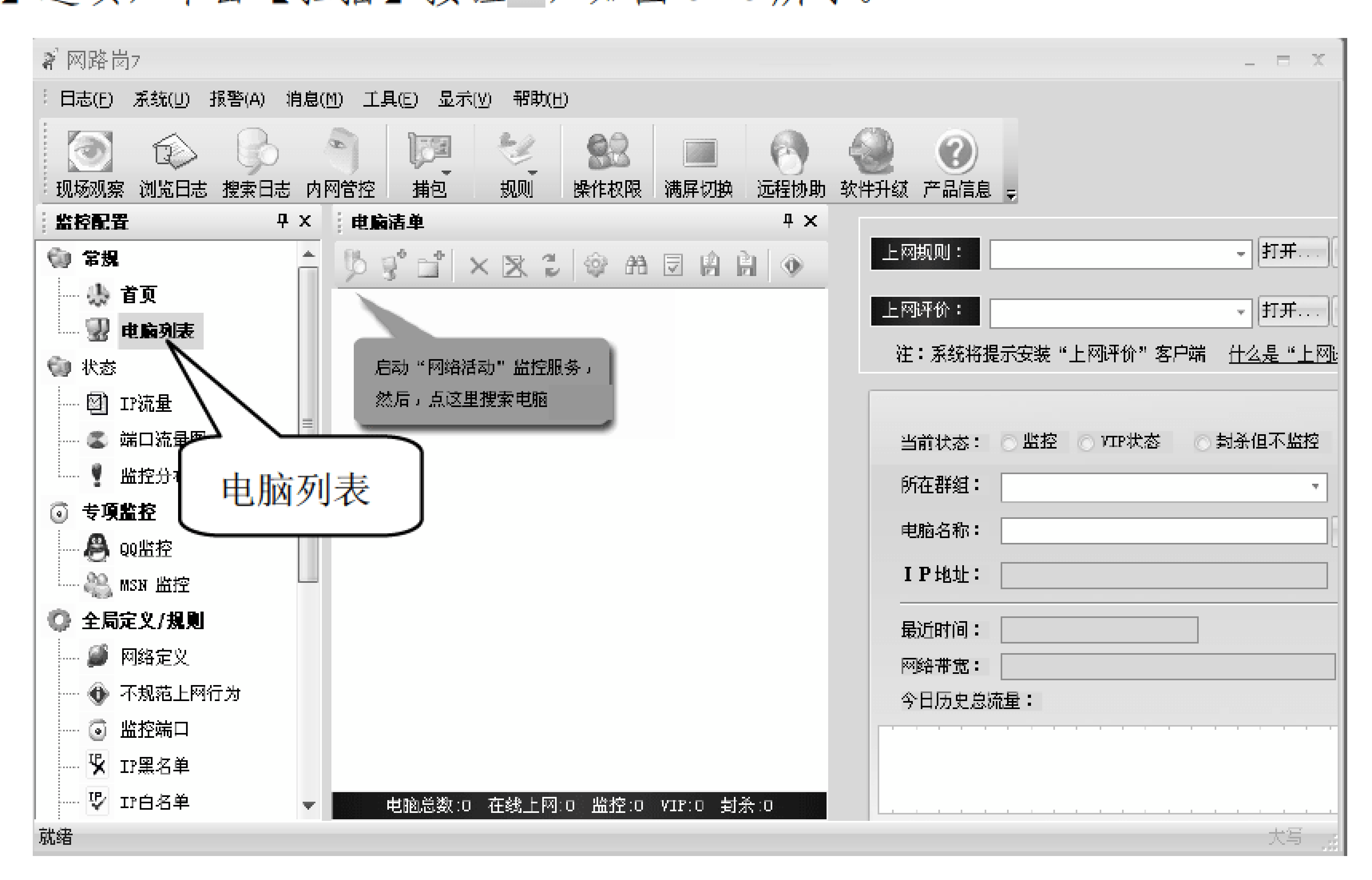


图 8-18

02 弹出【目标搜索】对话框，在【起始 IP】和【终止 IP】文本框中分别输入要搜索的内部网络的 IP 地址范围，本案例中在【起始 IP】和【终止 IP】文本框中分别输入 172.16.4.1 和 172.16.4.255，单击【开始搜索】按钮，如图 8-19 所示。



图 8-19

03 如图 8-20 所示，搜索正在进行中。



图 8-20

04 搜索完成后，返回至网路岗七代监管软件操作界面，并显示扫描到的计算机，如图 8-21 所示。



图 8-21

05 设置计算机的监测状态。如图 8-22 所示，选择要监控的计算机，然后在右侧选择【监控】单选按钮，单击【保存】按钮。

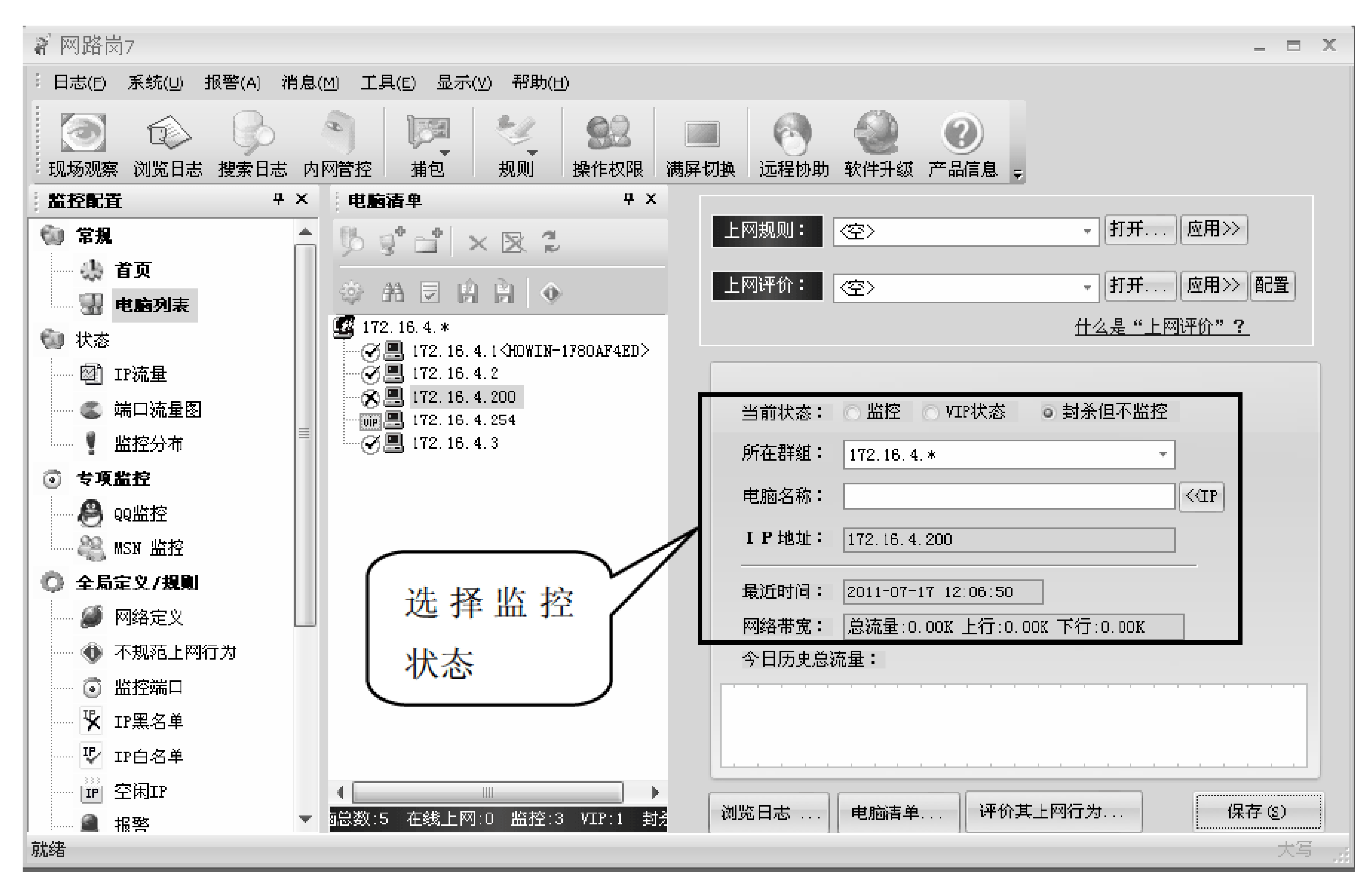


图 8-22

网路岗七代监管软件对计算机的监控状态有监控、VIP 监控和封杀但不监控三种，如图 8-22 所示。

（1）在计算机 IP 地址前面为【】表示严格监控。
（2）在计算机 IP 地址前面为【VIP】表示 VIP 监控，就是不监控。
（3）在计算机 IP 地址前面为【】表示直接封杀不监控。

8.3.4 监管员工的上网行为

使用网路岗七代监管软件，可以管理、控制内部员工的上网行为，下面主要介绍几种常用的上网行为监管设置。

1. 网页过滤

一般来说公司会允许员工访问一些常用网站，但是很多娱乐网站或者是一些非法网站是禁止员工访问的。通过设置访问规则，禁止员工访问非法网站的具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代监管软件的操作界面，单击左侧【电脑列表】选项，任意选择一台计算机，单击右侧【上网规则】右侧的【打开】按钮，如图 8-23 所示。

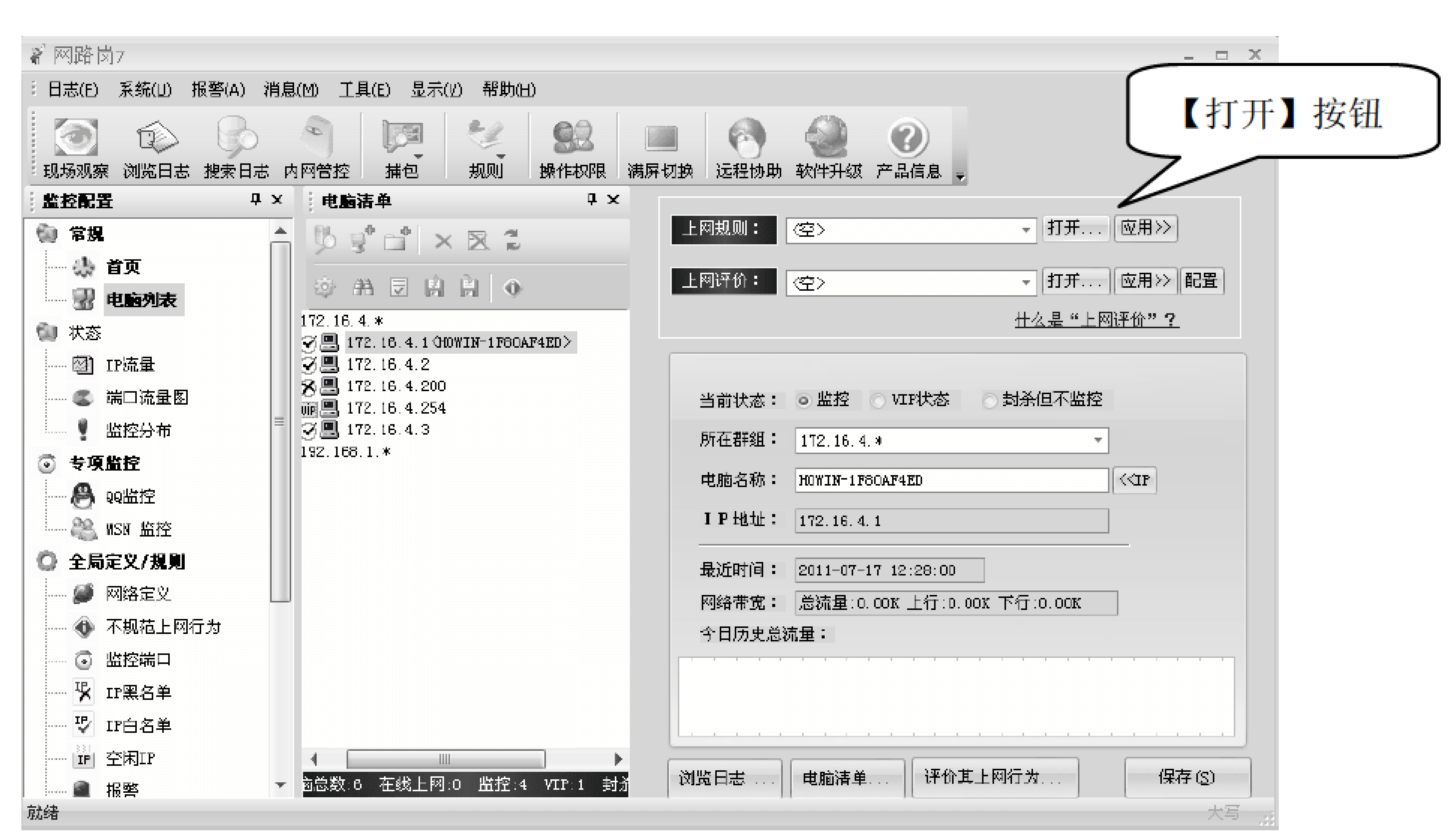


图 8-23

02 弹出【编辑“上网规则”】窗口，单击【添加规则】按钮，并将规则命名为【禁止员工访问娱乐网站】，如图 8-24 所示。

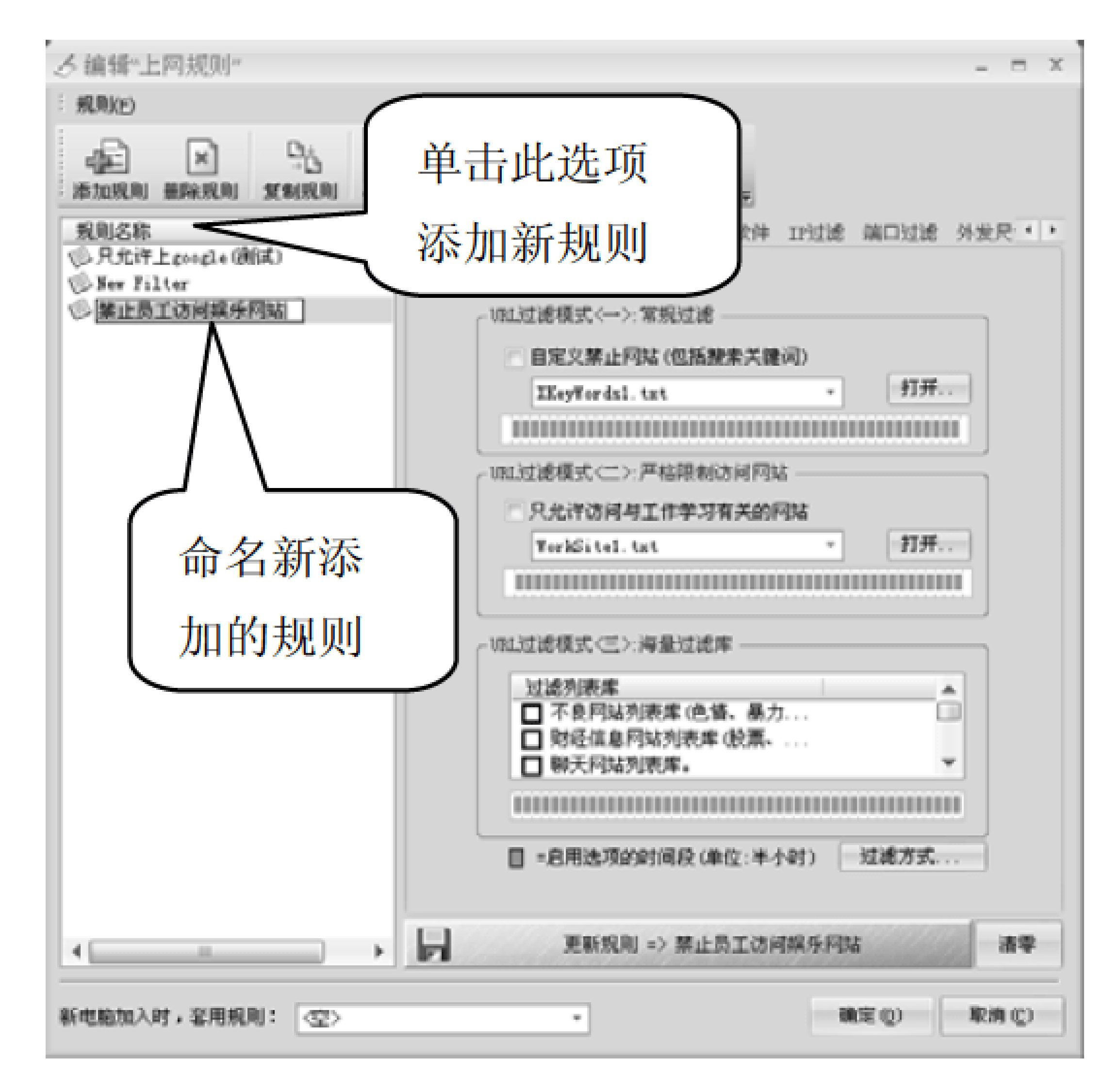


图 8-24

03 如果允许员工访问大部分网站，禁止个别非法网站，则选择【URL 过滤模式<一>：常规过滤】过滤模式。勾选【自定义禁止网站】复选框，单击【打开】按钮，如图 8-25 所示。



图 8-25

04 弹出过滤规则文件，在里面输入要禁止网站网址的关键字。比如本实例中笔者不允许内部员工访问 qq 空间，则 qq 空间网址中有一个关键字为 qzone，则将 qzone 写入该文件中，所有含有 qzone 字母的网址都打不开。当然本实例如下所示，添加了 qzone、xunlei、qq 等关键字。单击【保存】按钮，然后单击该文本右上角的【关闭】按钮 ☒，将该文本关掉，如图 8-26 所示。

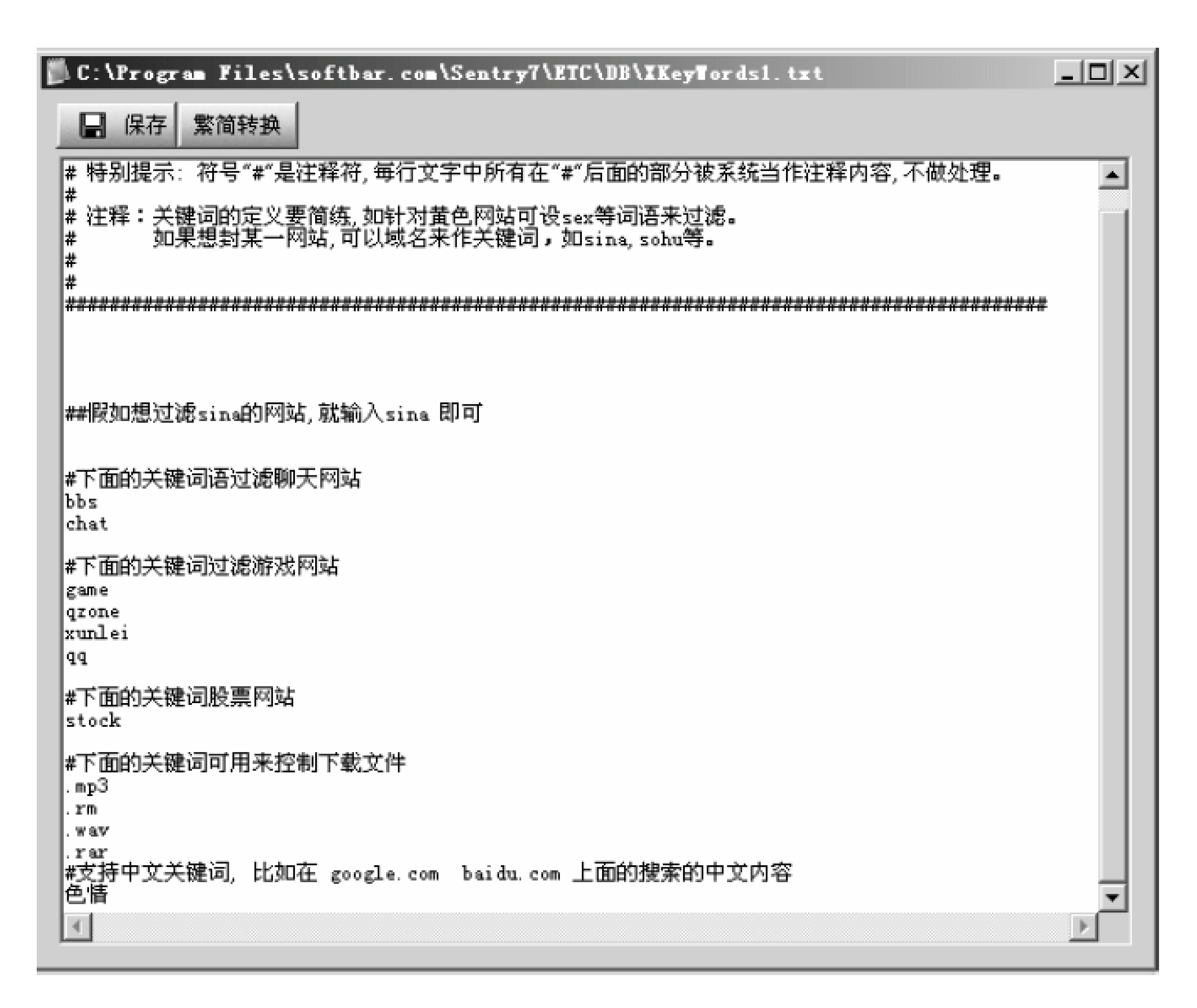


图 8-26

05 返回至【编辑“上网规则”】对话框，单击【更新规则=>禁止员工访问娱乐网站】按钮，然后单击【确定】按钮，完成上网规则的设置，如图 8-27 所示。



图 8-27

06 如果要制定更加严格的上网规则，只允许员工访问个别网站，其他的网站一律禁止，则可以使用【URL 过滤模式<二>: 严格限制访问网站】过滤模式。单击【添加规则】按钮，并将规

则命名为【允许员工访问公司网站】。勾选【只允许访问与工作学习有关的网站】复选框，单击【打开】按钮，如图 8-28 所示。



图 8-28

07 弹出规则设置文件，在该文件中添加需要打开的网站，注意只需要输入网站的域名即可。本实例中允许员工访问网易网页，则输入 163.com 即可。单击【保存】按钮，然后单击该文本右上角的【关闭】按钮 ☒，将该文本关掉，如图 8-29 所示。

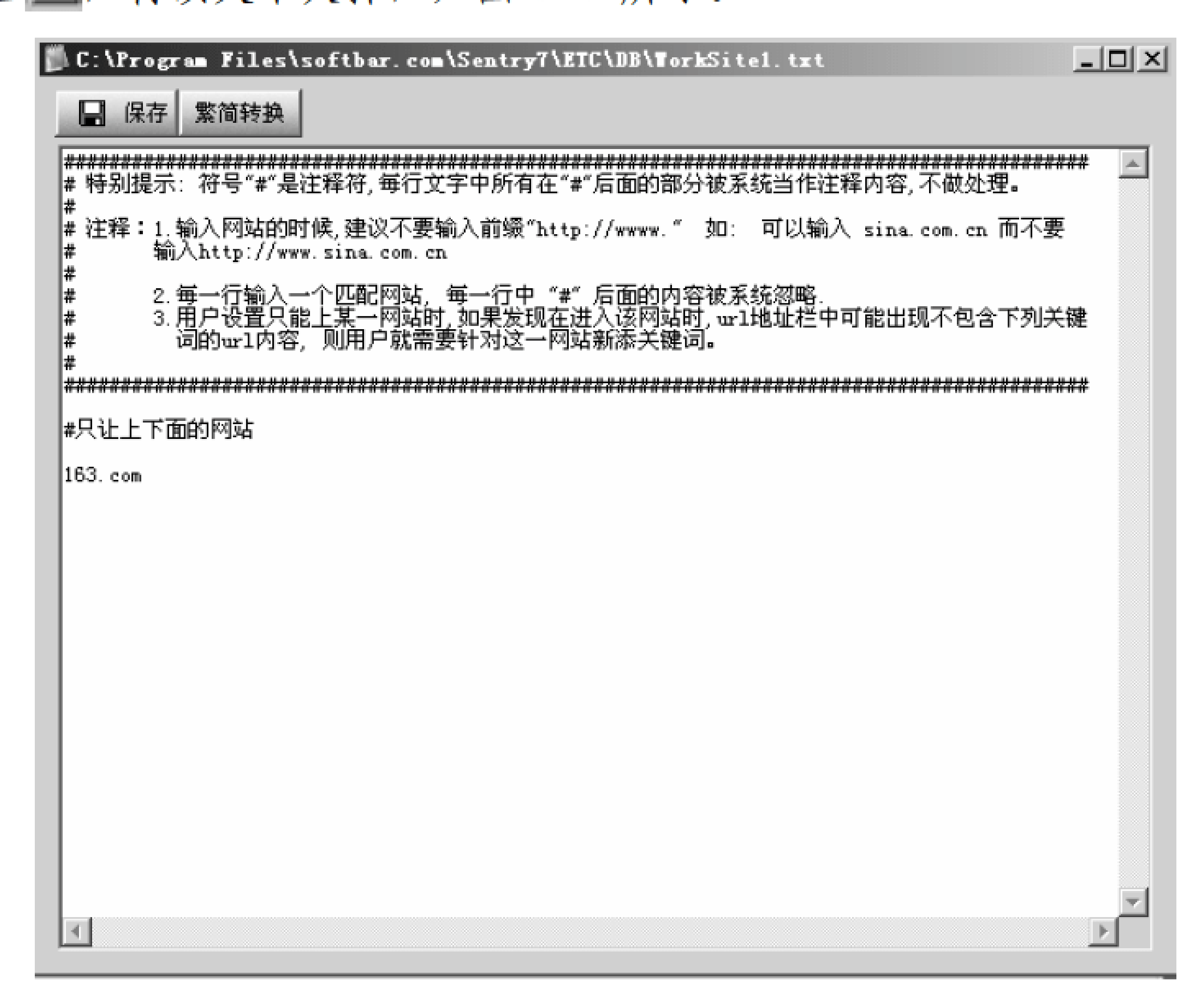


图 8-29

08 返回至【编辑“上网规则”】对话框，单击【更新规则=>允许员工访问公司网站】按钮，然后单击【确定】按钮，完成上网规则的设置，如图 8-30 所示。



图 8-30

09 返回至网路岗七代网络监管软件操作界面。选中要限制访问网站的计算机，本实例中笔者选择 IP 地址为 172.16.4.1 的计算机，然后单击【上网规则】下拉菜单，在弹出的下拉菜单中选择【禁止员工访问娱乐网站】规则文件，单击【保存】按钮，如图 8-31 所示。

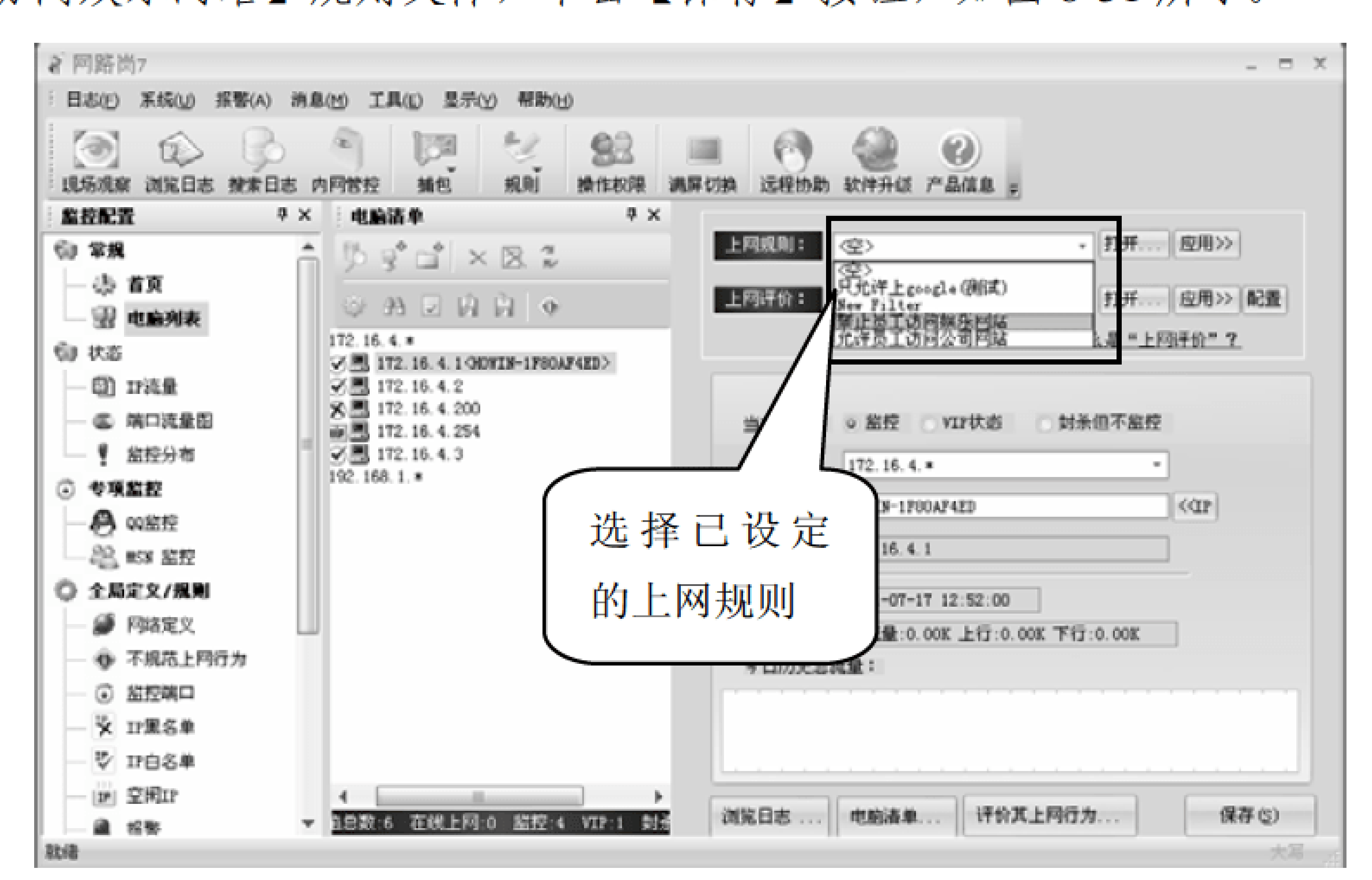


图 8-31

10 返回至网路岗七代网络监管软件操作界面，此时 IP 地址为 172.16.4.1 的计算机就会受到上网规则的限制，如图 8-32 所示。



图 8-32

2. 禁止 BT、P2P 等下载

随着 BT、P2P 的流行，员工在上班时间进行资源下载，往往会造成网络带宽的极大浪费，甚至影响到其他员工正常的网络访问，因此必须对网络下载进行限制。

使用网路岗七代网络监管软件进行下载限制的具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代网络监管软件的操作界面，单击左侧【电脑列表】选项，任意选择一台计算机，单击右侧【上网规则】后面的【打开】按钮，如图 8-33 所示。



图 8-33

02 弹出【编辑“上网规则”】对话框，单击【添加规则】选项，并将规则命名为【禁止员工进行下载】，如图 8-34 所示。



图 8-34

03 选择【流量限制】选项卡，选择【限制上行和下行流量】单选按钮，在【上行】和【下行】文本框中分别输入要限制的带宽。本实例中限制上行带宽为 30KB，下行带宽为 80KB，如图 8-35 所示。



图 8-35

04 选择【下载类型】选项卡，在【禁止下载下列类型文件】选项列表中勾选不允许员工下载文件的类型。如果某些文件类型不在该列表中，可以单击【添加】按钮进行添加。设置完成后，单击【更新规则=>禁止员工进行下载】按钮，然后单击【确定】按钮，如图 8-36 所示。

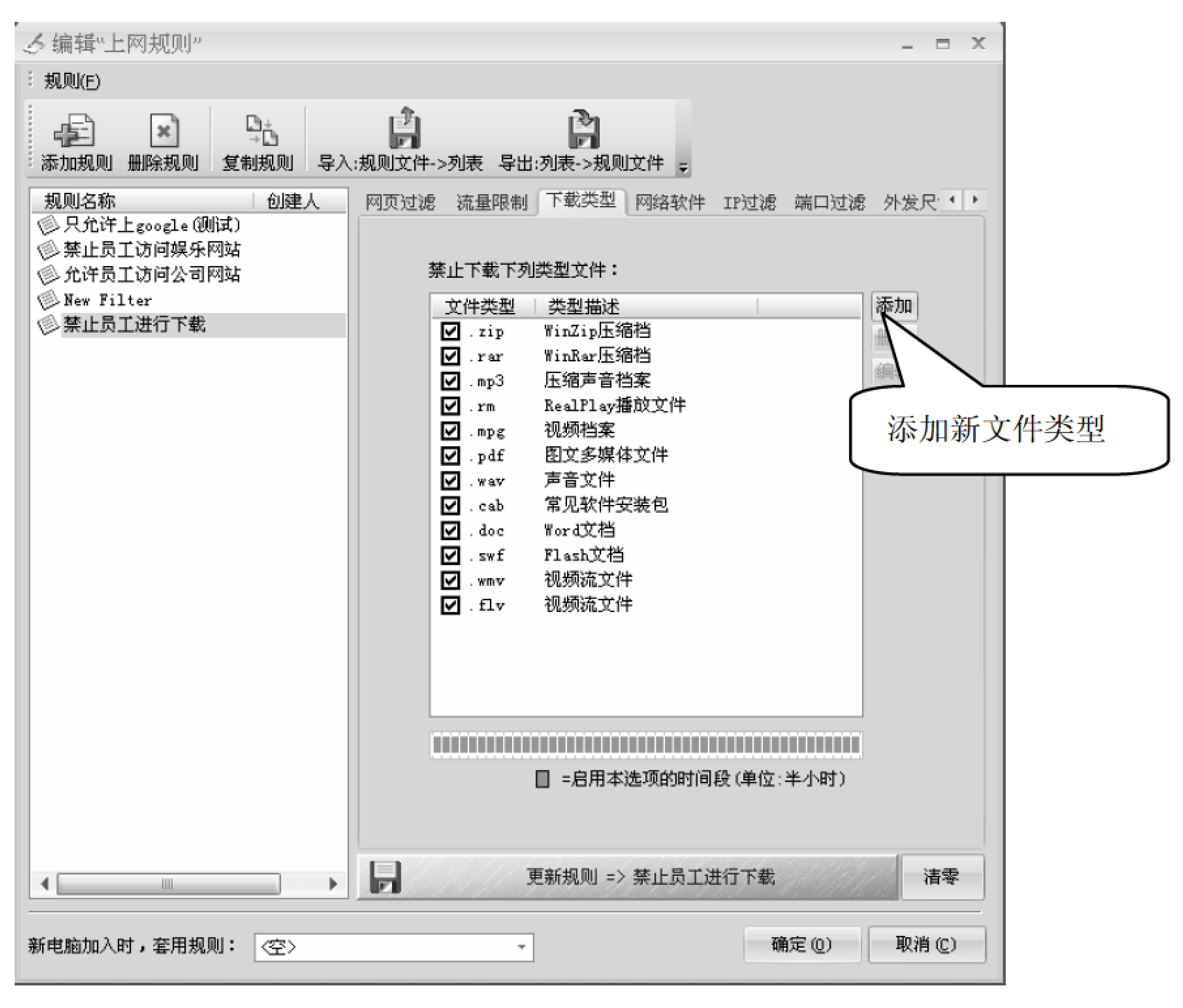


图 8-36

05 返回至网路岗七代网络监管软件操作界面。选中要进行下载限制的计算机 IP 地址，本实选择 IP 地址为 172.16.4.1 的计算机。然后单击【上网规则】下拉菜单，在弹出的下拉菜单中选择【禁止员工进行下载】上网规则，单击【确定】按钮，如图 8-37 所示。



图 8-37

06 返回至网路岗七代网络监管工具操作界面，此时 IP 地址为 172.16.4.1 的计算机将不能进行下载，如图 8-38 所示。



图 8-38

3. 使用全局规则设定简化管理

在上面的讲解中可以针对网络内部的用户进行上网行为控制，但是很多规则往往针对网络中的每一个员工，这时候可以利用全局规则设定。

配置全局规则的具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代网络监管软件的操作界面，单击左侧【全局定义/规则】选项下的【不规范上网行为】选项，如图 8-39 所示。

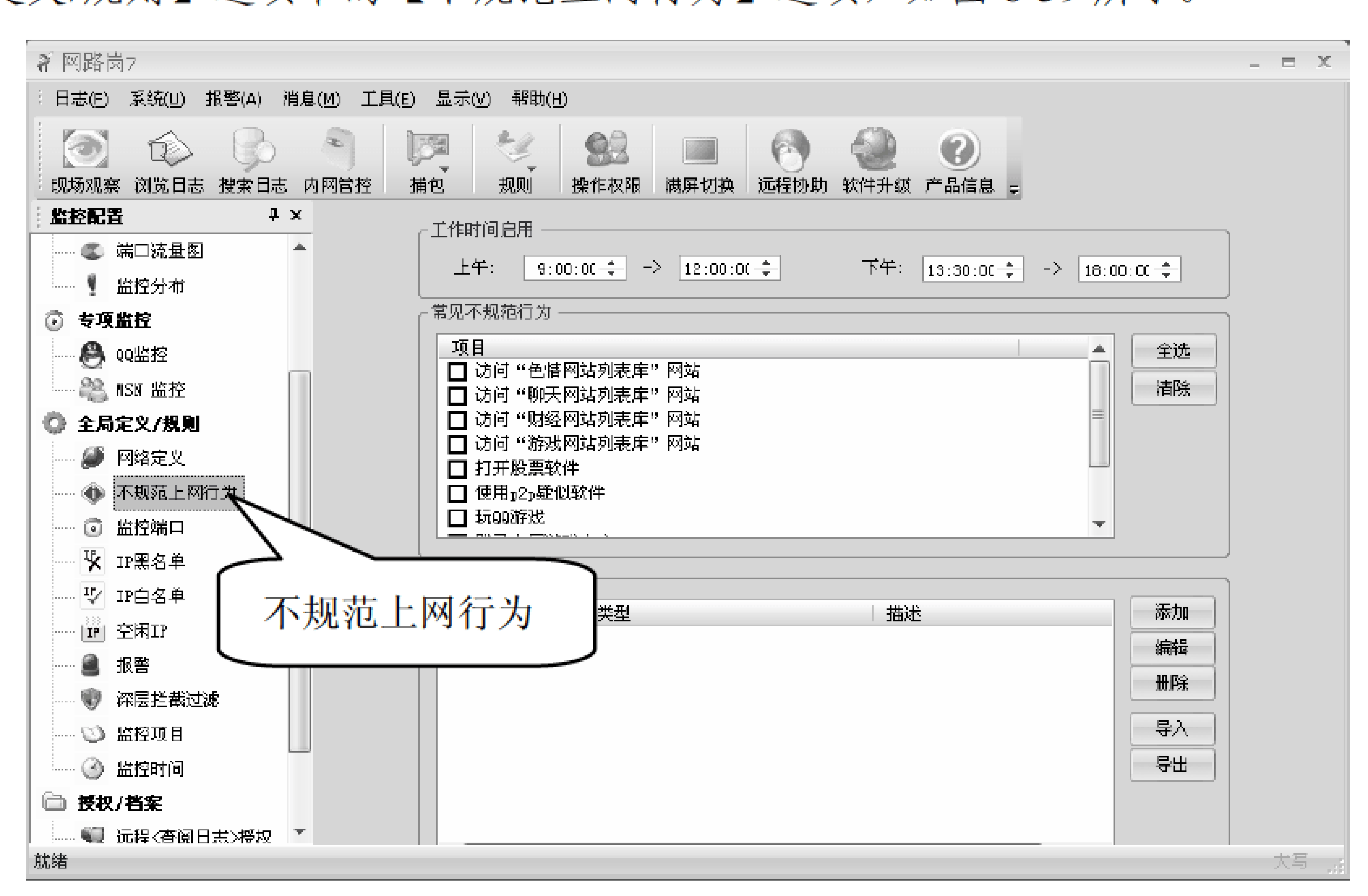


图 8-39

02 在【工作时间启用】选项下方的【上午】和【下午】文本框中分别输入启用该规则的时间。本实例输入工作时间为上午 8:30-12:00，下午为 14:00-18:00，在【常见不规范行为】选项中勾选【使用 p2p 疑似软件】和【玩 QQ 游戏】复选框，单击【添加】按钮，如图 8-40 所示。

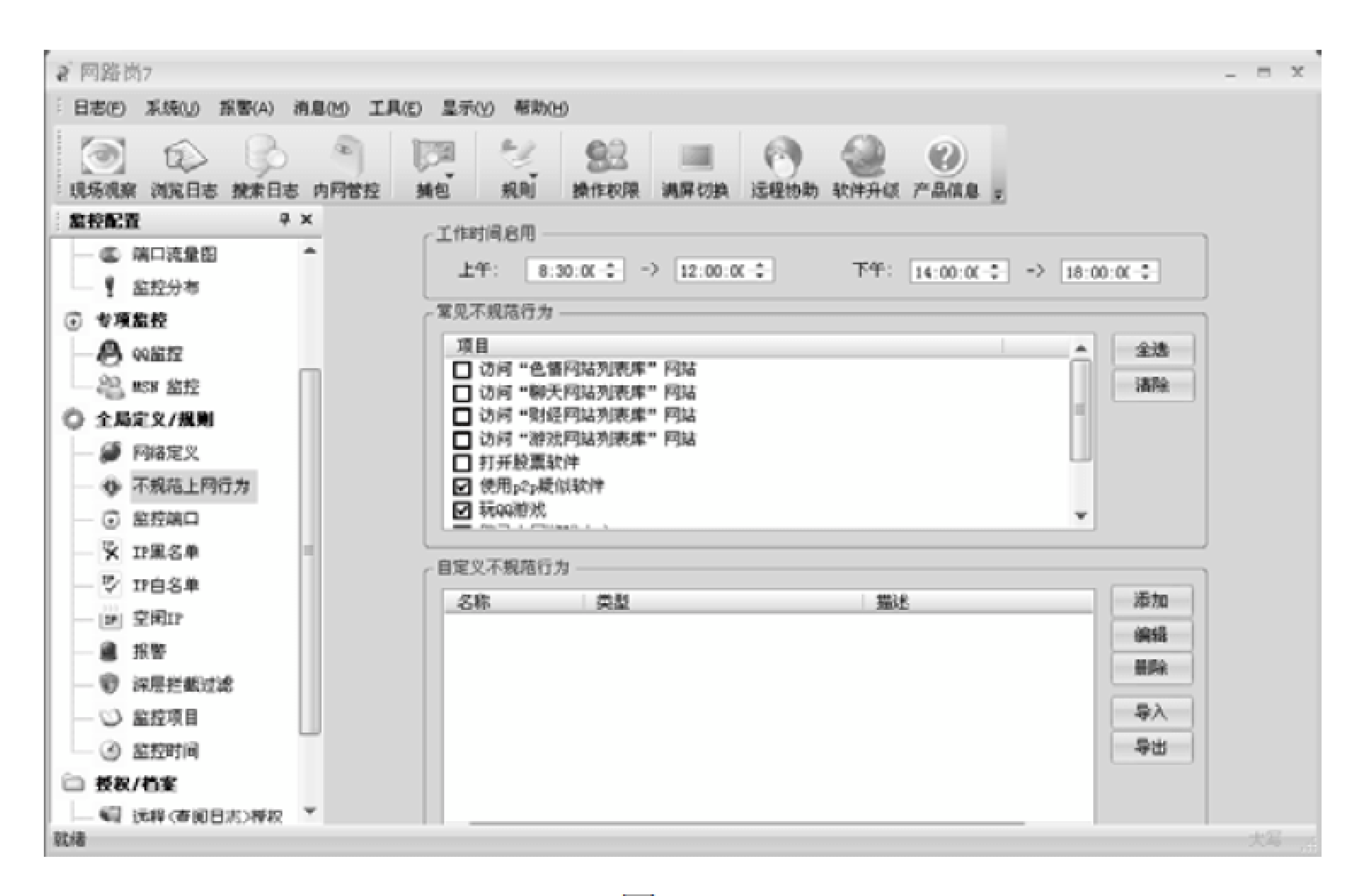


图 8-40

03 弹出【自定义项目】对话框，在【报警类型】下拉菜单中选择【访问敏感网站】，在【报警名称】文本框中输入【禁止访问娱乐网站】，在【访问网站的 URL 包含下面的关键词：】文本框中输入禁止所有员工访问网站域名的关键词。本实例中禁止员工访问含有 qzone、download 的网站，单击【确定】按钮，如图 8-41 所示。

图 8-41

04 返回至网路岗七代网络监管软件操作界面，勾选【禁止访问娱乐网站】复选框。单击【保存设置】按钮，如图 8-42 所示。



图 8-42

05 弹出【询问】提示框，单击【是】按钮，如图 8-43 所示。



图 8-43

此时，针对网络内部的全部上网规则设置完成。网络内部所有员工访问互联网都要受到该规则的限制。

8.3.5 监测用户数据流量

用户在访问网站和下载资源的时候都会产生网络流量，对网络流量的分析有助于了解当前网络带宽是否满足办公需求，对员工个人数据流量的分析有助于更好的对员工的上网行为进行监管。

监测用户数据流量的具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代网络监管工具的操作界面，单击左侧【状态】➢【IP 流量】选项。如图 8-44 所示，在上面会看到当前网络数据流量大小，在下面会看到网络中每个计算机的当前流量和总流量。

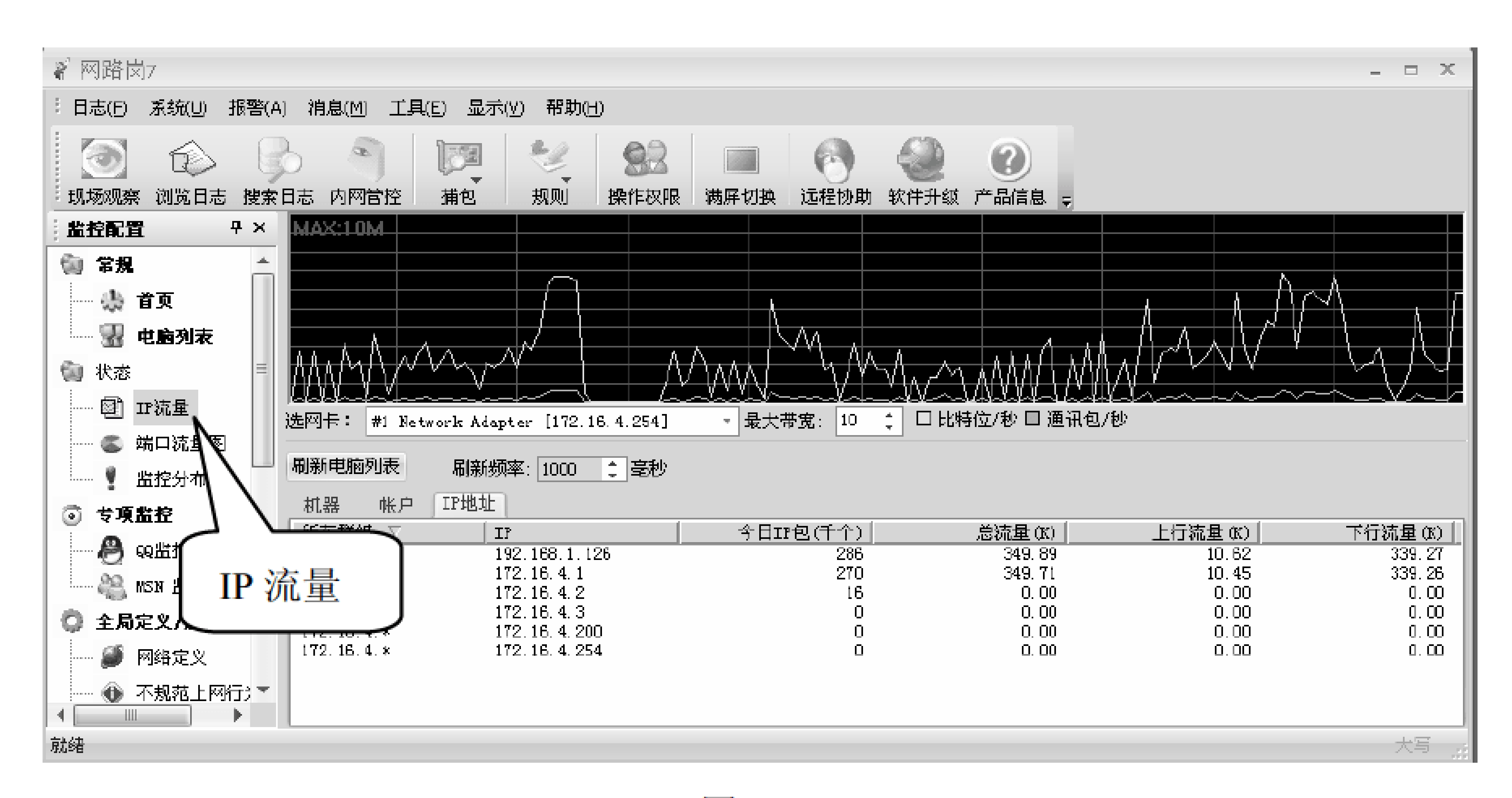


图 8-44

02 单击左侧【端口流量图】，可以看到网络中各种协议的使用比例，如图 8-45 所示，有助于网络管理员分析网络故障。

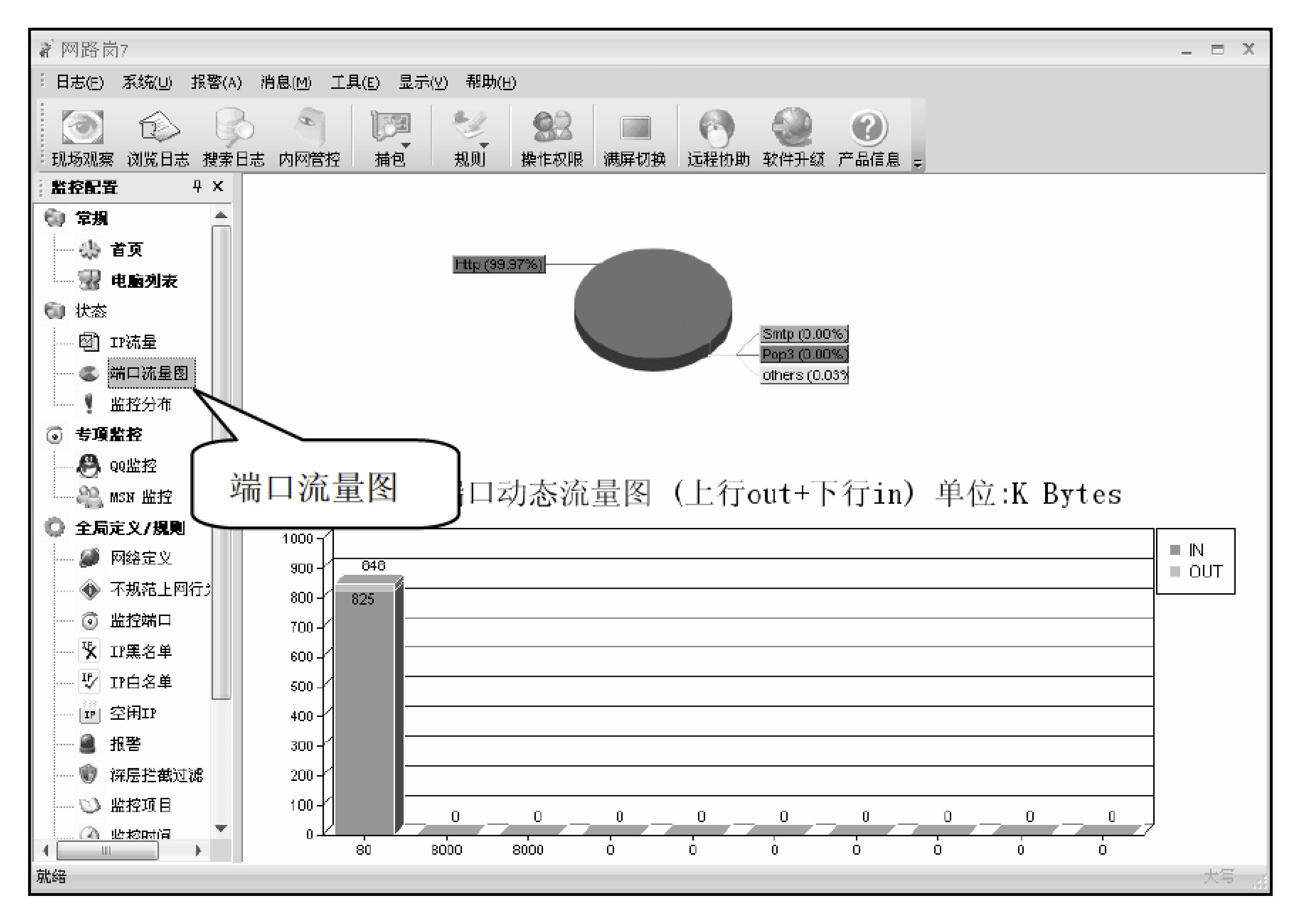


图 8-45

8.3.6　查找网络故障的原因

当网络出现故障后，首要要分析网络故障的原因，而网路岗七代网络监管工具的日志文件能够很好地帮助管理员进行故障分析，日志文件详细登记了网络用户的上网细则。

下面详细介绍如何通过查看网路岗七代日志来掌握网络用户上网的细则以及查看用户计算机的软硬件使用情况。

1. 现场观察

通过现场观察可以实时检测客户机上网情况，具体操作步骤如下。

01 双击桌面上的【网路岗 7】快捷方式，打开网路岗七代网络监管工具的操作界面，单击工具栏【现场观察】选项，如图 8-46 所示。



图 8-46

02 弹出【现场观察】窗口，在【监控动态】选项卡中可以看到当前客户机正在访问哪些网页，如图 8-47 所示。

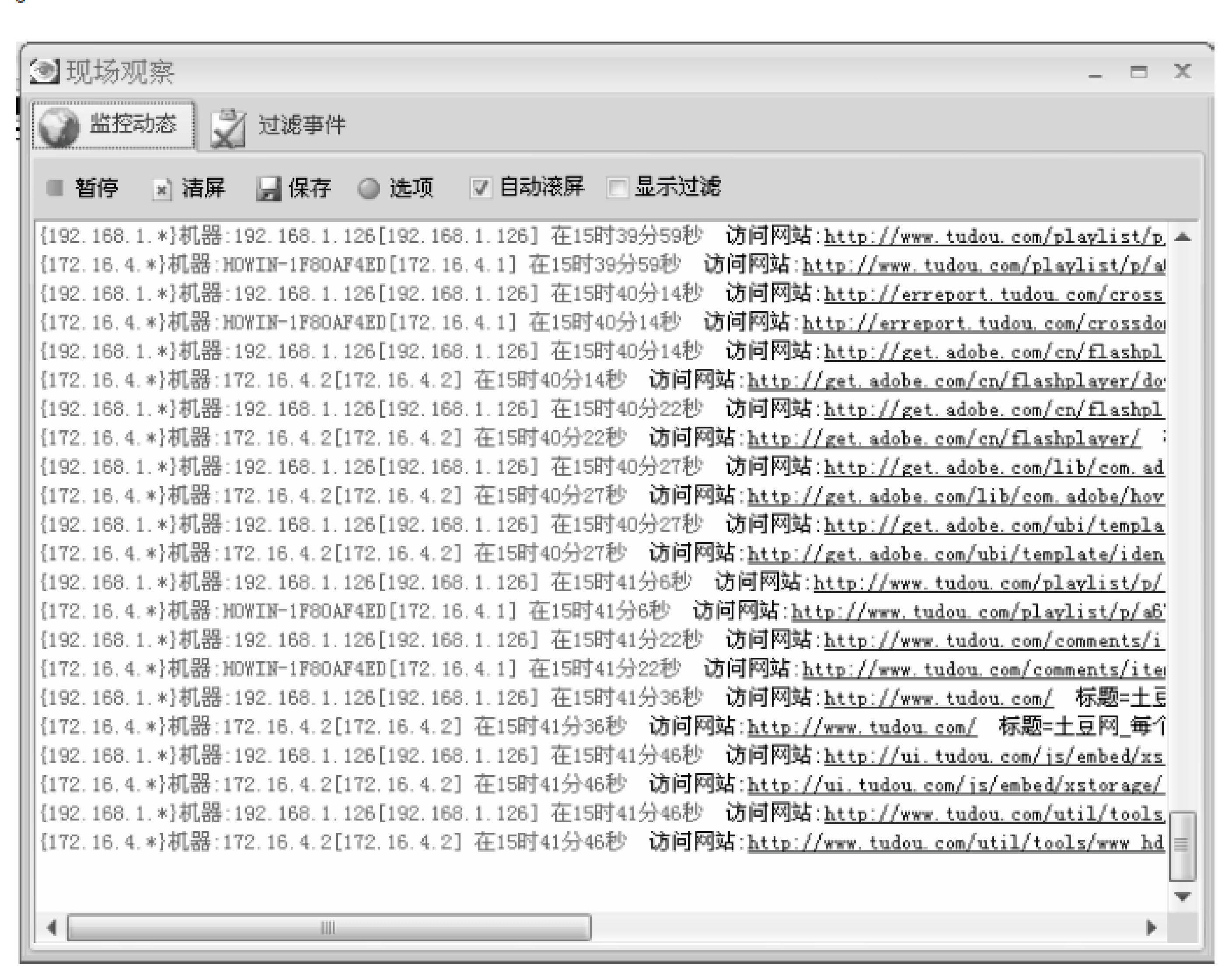


图 8-47

03 选择【过滤事件】选项卡，可以看到网路岗根据上网规则过滤掉的客户机访问的网页情况，如图 8-48 所示。

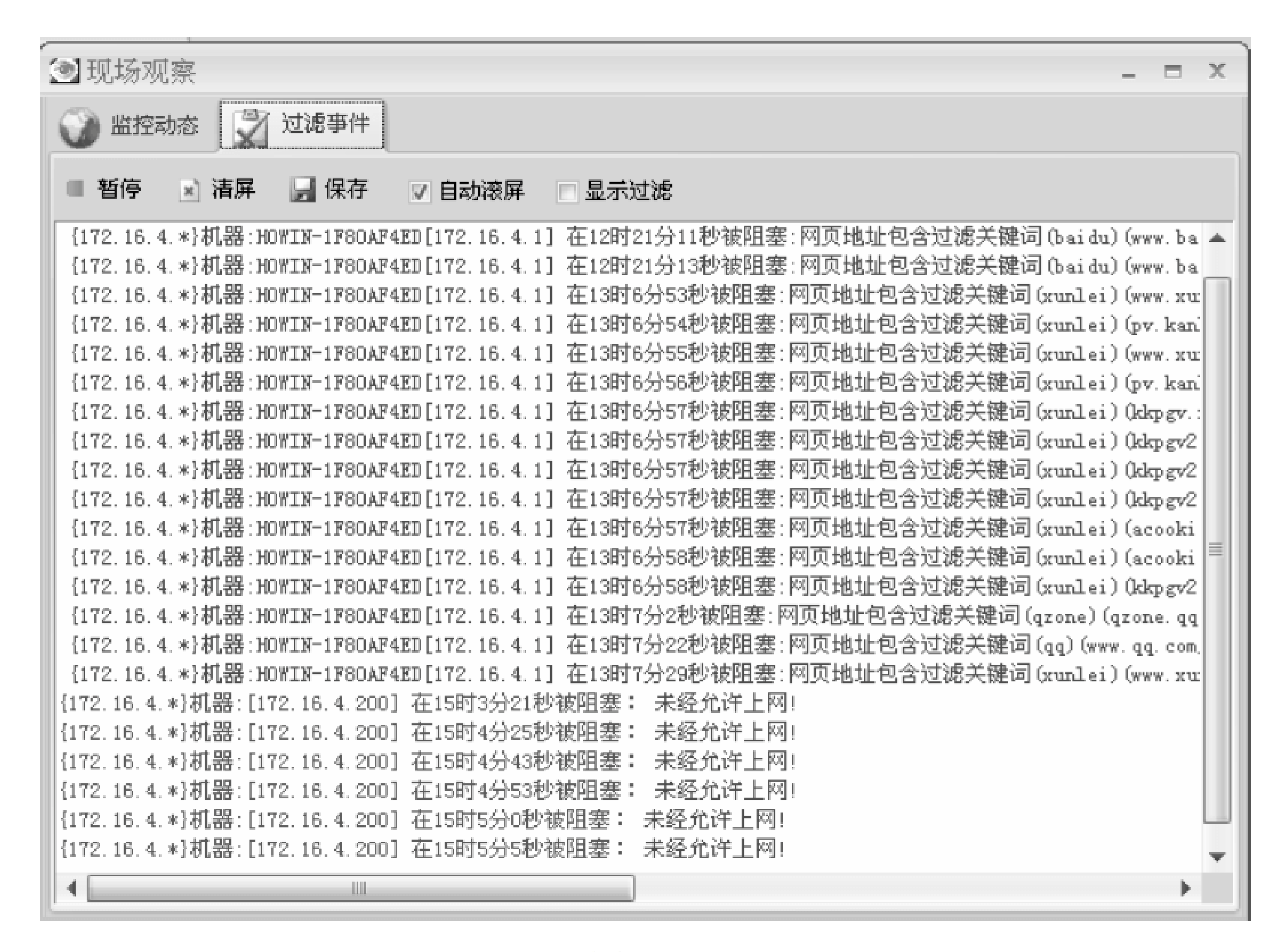


图 8-48

2. 浏览日志

通过【浏览日志】，可以查看客户机网络访问日志信息，具体操作步骤如下。

01 打开网路岗七代网络监管工具的操作界面，单击工具栏【浏览日志】选项，如图 8-49 所示。



图 8-49

02 打开【日志浏览器】窗口，如图 8-50 所示，可以看到网络内部计算机的所有上网行为。

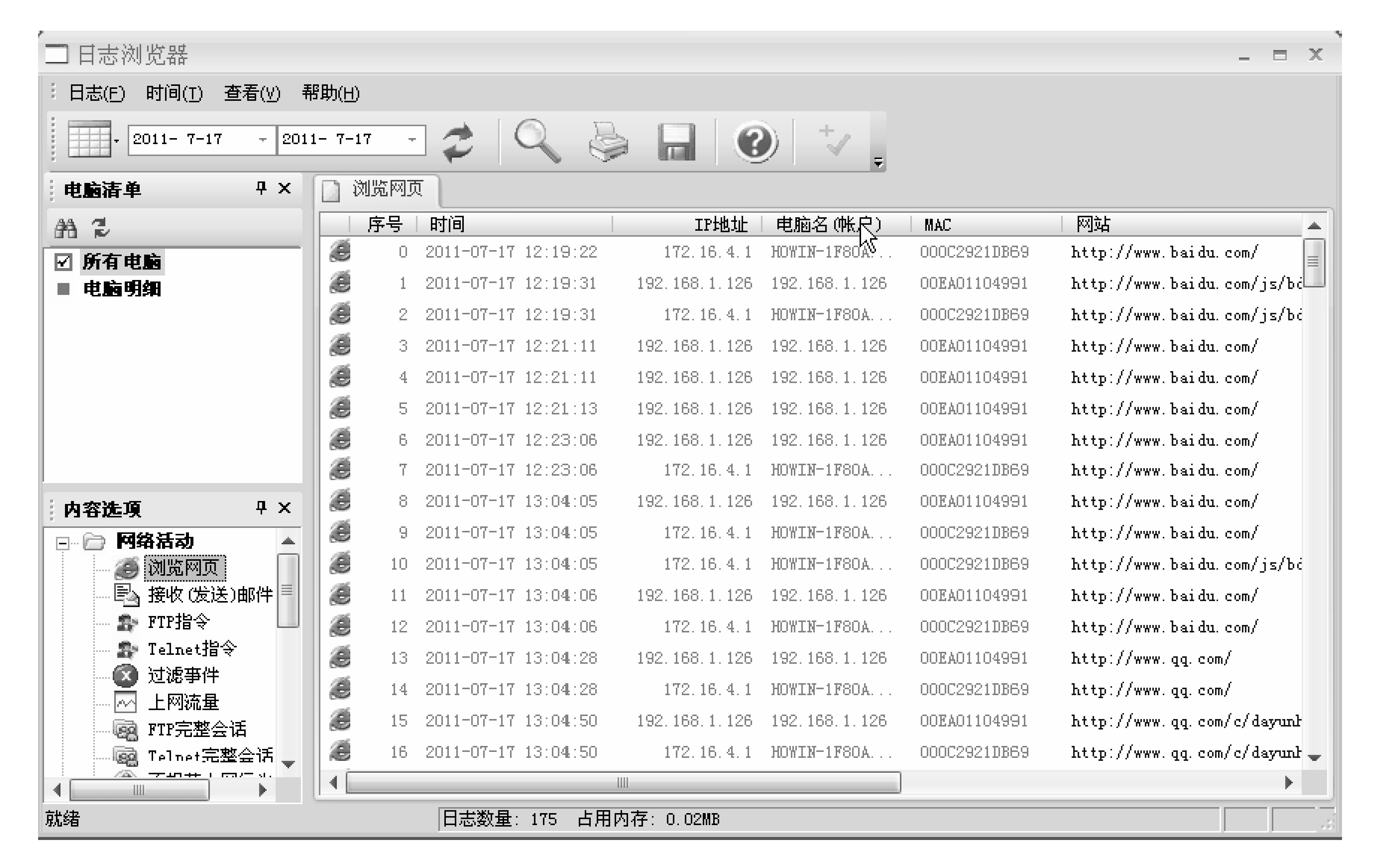


图 8-50

03 单击【电脑明细】➢【172.16.4.*】➢【172.16.4.1】选项，可以看到 IP 地址为 172.16.4.1 计算机访问网页的情况，如图 8-51 所示。

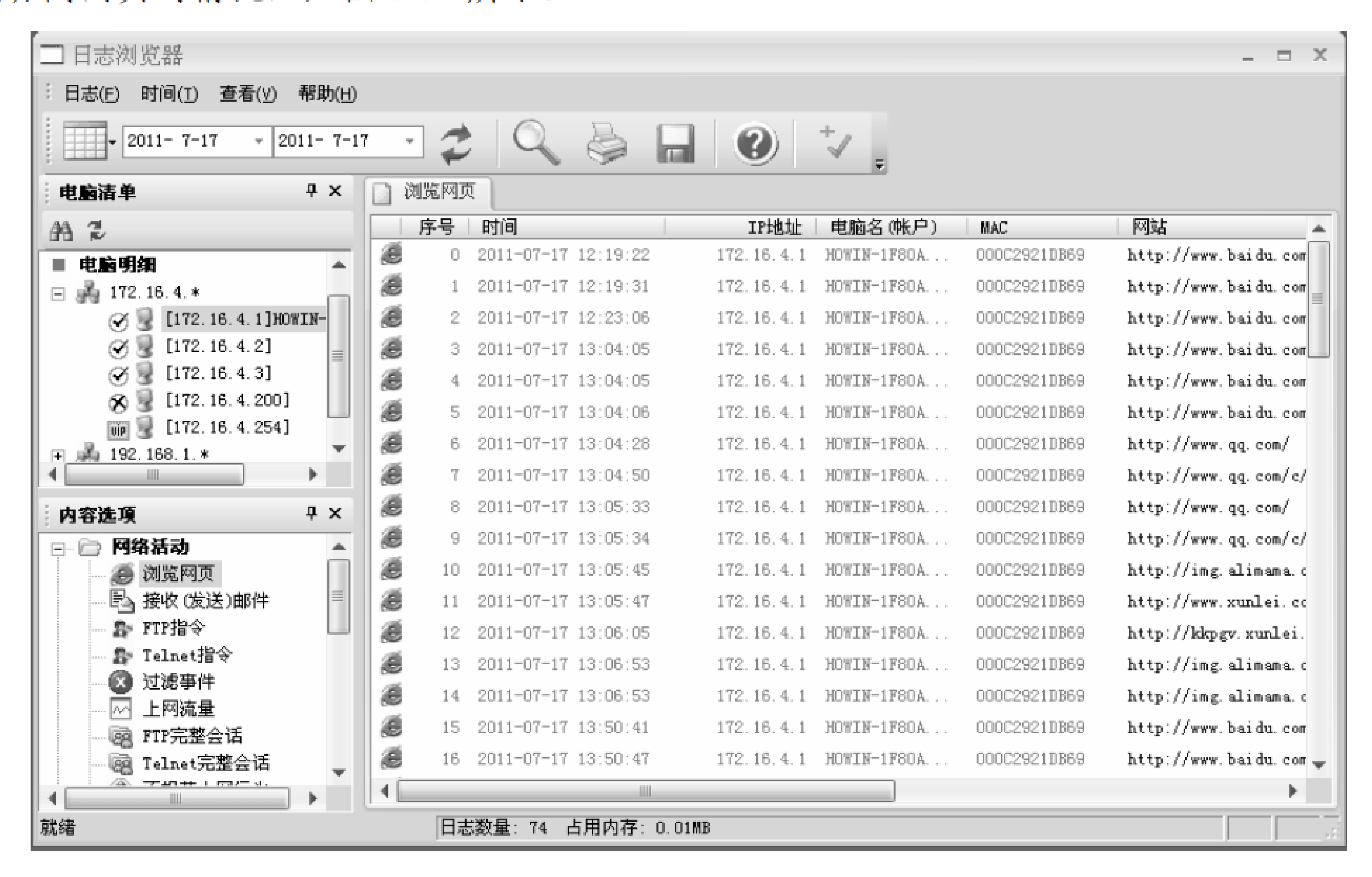


图 8-51

04 如果要看某个计算机的其他上网行为，可以在下面【内容选项】窗口中进行相应的选择，比如要查看 IP 地址为 172.16.4.1 的计算机的上网流量，单击左下方的【上网流量】选项就可以看到，如图 8-52 所示可以看到 1 个小时统计 1 次的网络数据流量。

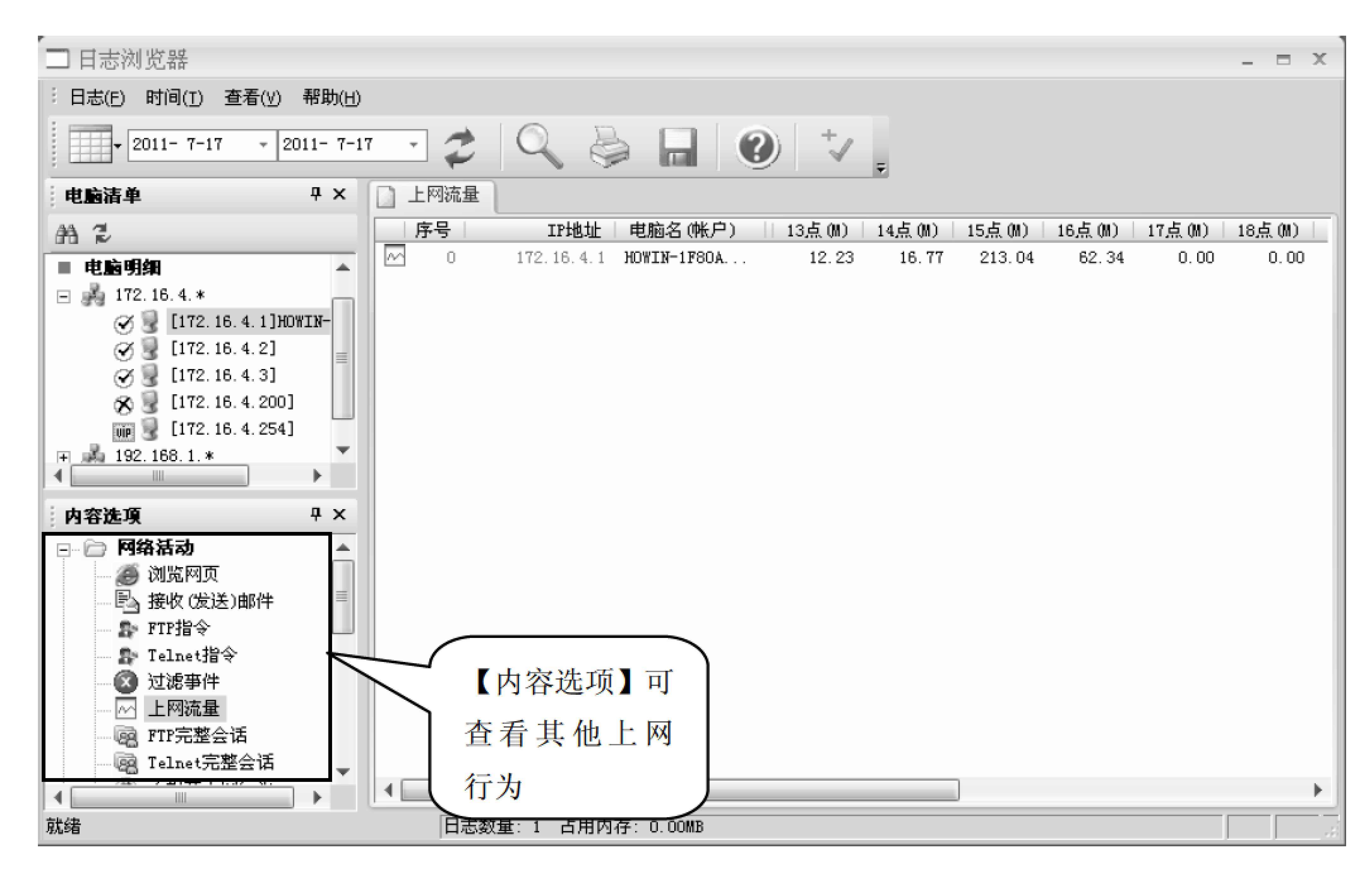


图 8-52

3. 管控内网客户机

通过【内网管控】可以查看内网的系统信息，具体操作步骤如下。

01 打开网路岗七代网络监管工具的操作界面，单击工具栏【内网管控】选项，如图 8-53 所示。



图 8-53

02 打开【内网管控】窗口，如图 8-54 所示，可以看到网络内部计算机的相关系统信息。

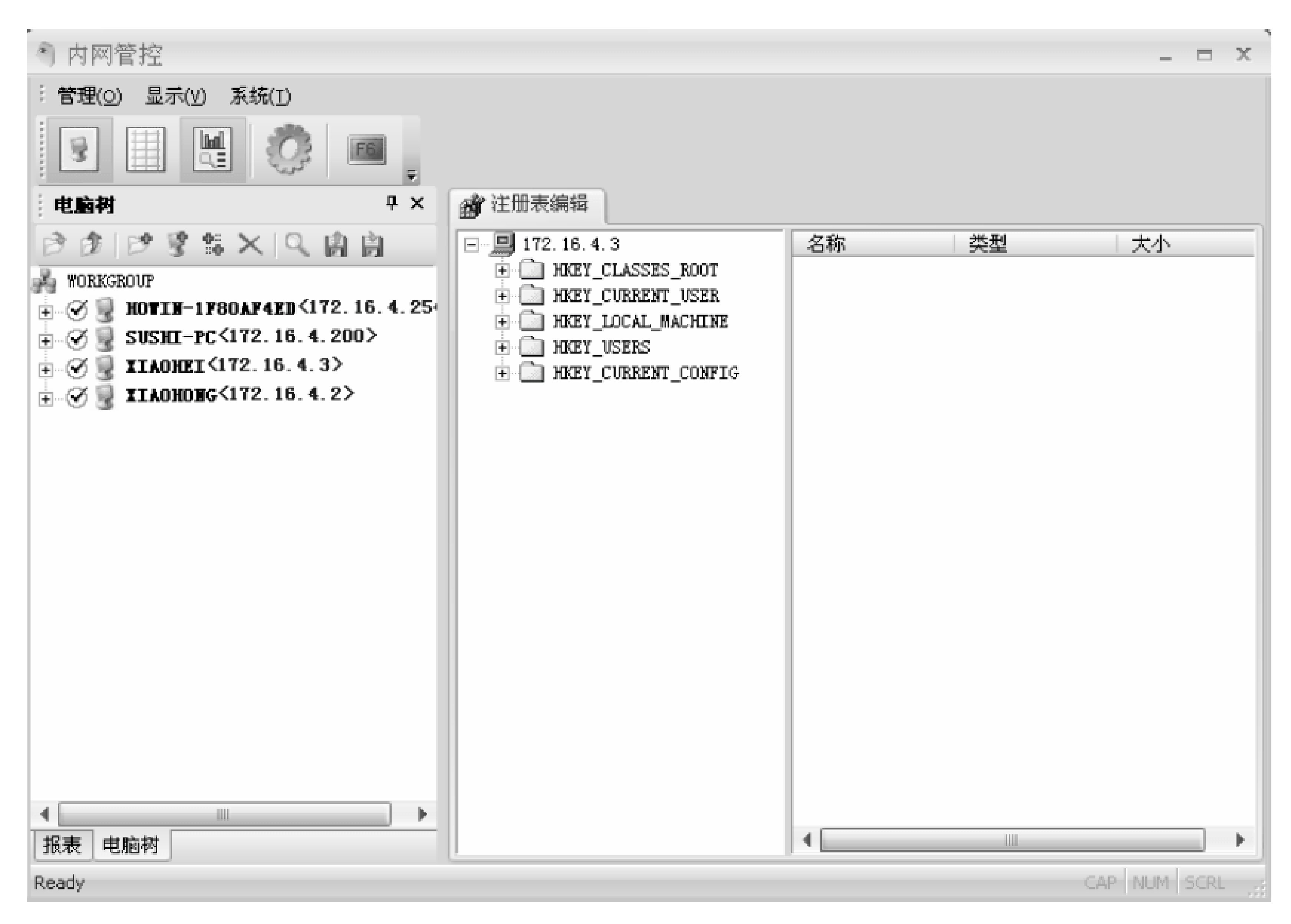


图 8-54

03 双击【172.16.4.3】➢【注册表编辑】选项，如图 8-55 所示可以看到 IP 地址为 172.16.4.3 的计算机的注册表信息。

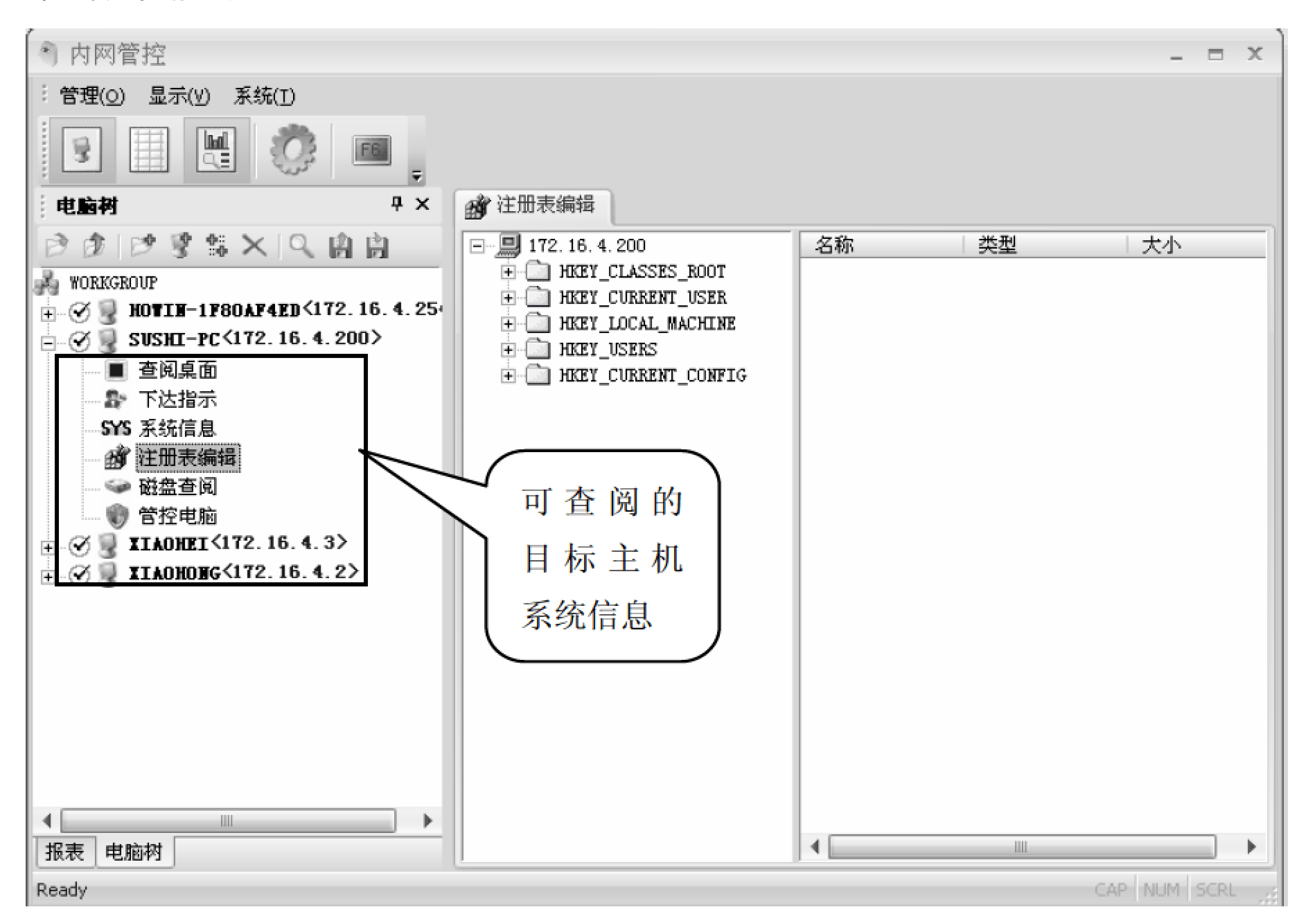


图 8-55

04 双击【172.16.4.3】➢【磁盘查阅】选项，如图 8-56 所示可以看到 IP 地址为 172.16.4.3 的计算机的硬盘使用信息。

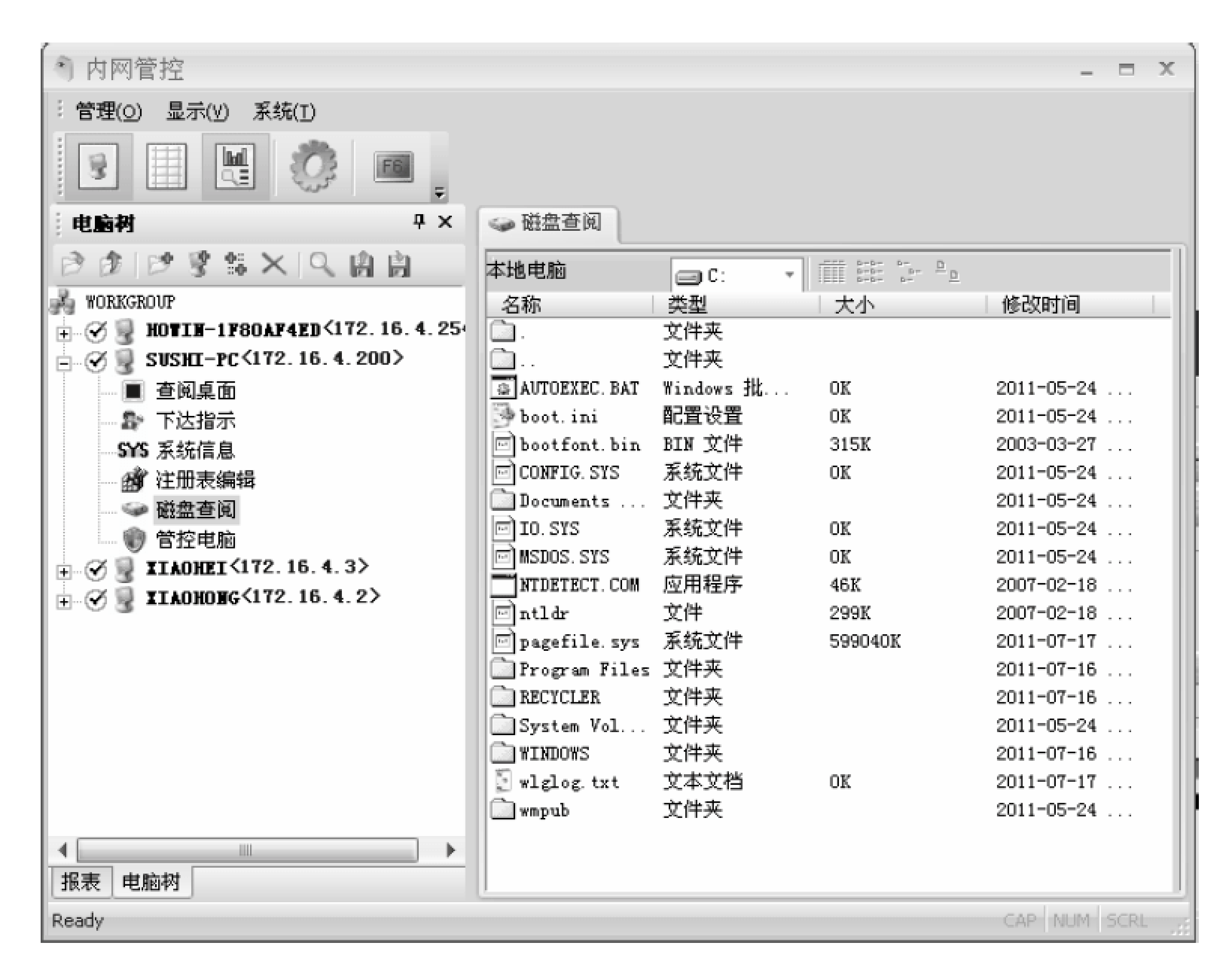


图 8-56



如果想要使用其他功能，比如【查阅桌面】、【下达指示】等，需要在网络内部计算机上安装网路岗七代网络监管工具的客户端程序。

8.4　专家答疑

（1）安装完网路岗后，进行计算机的扫描，计算机的监测状态是【VIP 监控】。如果手动更改为【监控】，网路岗软件又会自动更改为【VIP 监控】，导致不能正常使用，这是什么原因？

答：安装完网路岗七代网络监管工具后，首先需要进行注册后才能正常使用，否则会出现不能监控网络的情况。如果仅仅是为了做实验，可以在网路岗七代的官方网站申请注册号。

（2）网路岗七代有一个新的功能是捕捉网络数据包，我已经设置好了监控网卡，可是捕捉不到任何数据包，怎么解决？

答：如果要使用网路岗七代网络监管工具捕捉数据包，则需要安装 Winpcap 驱动。

（3）网路岗七代有一个新的功能是可以捕捉到客户端的桌面，要对客户端的桌面进行快照捕捉，怎么实现？

答：如果要使用网路岗七代网络监管工具的桌面捕捉功能，则需要在客户端安装客户端程序，安装完成后连接服务器端，之后就可以在服务器端查阅客户端的桌面。

第 9 章　网络安全基础

网络发展至今，人们关注的已经不仅仅是网络能否满足业务需求，更关注的是能否安全的、可靠的完成业务需求。这是因为网络安全事件频繁发生，网络安全威胁无处不在，因网络安全造成的损失难以控制。

网络安全技术在这样的环境下越来越受重视，技术发展水平也越来越高。下面将详细介绍网络安全技术概述、网络安全威胁类型、网络安全解决办法等内容。

9.1　网络安全的概述

和网络安全相关的很多名词另大家印象深刻，比如病毒、木马、系统漏洞、网络攻击等。但到底什么是网络安全，它的特征又是什么？很多人无法给出准确、完整的描述。作为网络安全工程师，在实施网络安全架构和管理时必须要完整的认识网络安全，否则很容易构建出不完善的网络架构。

9.1.1　网络安全的概念

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的因素而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。

网络安全最重点保护的不是硬件、软件本身，而是所有网络中的信息。这个信息没有明确的定义，网络中任何有价值的信息都在保护之列。网络安全的实现涉及到了计算机科学、网络技术、信息安全技术、密码技术、通信技术、应用数学、数论、信息论等多方面的知识，是一个综合性的技术体系。

实现网络安全主要用到的技术手段有防火墙、IDS 入侵检测、防毒墙、流量监测分析、VPN、CA 认证、访问控制列表、Qos 服务质量等。每一项技术手段都可以满足一定的网络安全需求。如防火墙用于安全隔离内网，IDS 用于扫描网络攻击，防毒墙用于企业反病毒，CA 用于提供安全加密身份认证、访问控制用于实现网络流量控制。无论是哪种技术手段，最终的目的都是为了确保网络的可用性、完整性和保密性。

9.1.2　网络攻击类型

目前，网络攻击模式呈现多方位、多手段化，让人防不胜防。网络攻击的实质就是利用被攻击方信息系统自身存在的安全漏洞，通过使用网络命令和专用软件进入对方网络系统的攻击。目前

网络攻击的类型主要有以下几种。

- 利用监听嗅探技术获取对方网络上传输的有用信息。
- 利用拒绝服务攻击使目的网络暂时或永久性瘫痪。
- 利用网络协议上存在的漏洞进行网络攻击。
- 利用系统漏洞，例如缓冲区溢出或格式化字符串等，以获得目的主机的控制权。
- 利用网络数据库存在的安全漏洞，获取或破坏对方重要数据。
- 利用计算机病毒传播快、破坏范围广的特性，开发合适的病毒破坏对方网络。

9.1.3 网络安全的威胁

计算机网络发展至今，计算机病毒、网络攻击等严重影响了网络应用。作为网络使用者、维护者，必须直面以对，及早做出防范。

下面介绍几种常见的网络安全威胁。

1. 威胁个人网络隐私

计算机网络有很多默认的记录功能，会将用户的很多网络访问信息、系统操作信息进行登记，主要以缓存和历史记录方式存在。如果不及时清理这些信息，很容易被网络攻击者利用，危害个人隐私安全。

很多网络攻击者，可以通过网络攻击登录用户操作系统查看缓存和历史记录信息，同时也可以将有操作记录功能的木马程序散播入互联网，被感染的用户的所有计算机使用情况都会被记录、窃取。

一般可以直接操作系统删除缓存和历史记录信息，也可以使用专门的系统优化工具清理。对于植入的木马可以使用专门的木马、插件扫描工具清理。

例如，可以通过以下步骤清理 IE 缓存和历史记录信息。

01 在桌面右击【Internet Explorer 浏览器】图标，在弹出的快捷菜单中选择【属性】菜单命令，弹出【Internet 属性】对话框，单击【删除】按钮，如图 9-1 所示。

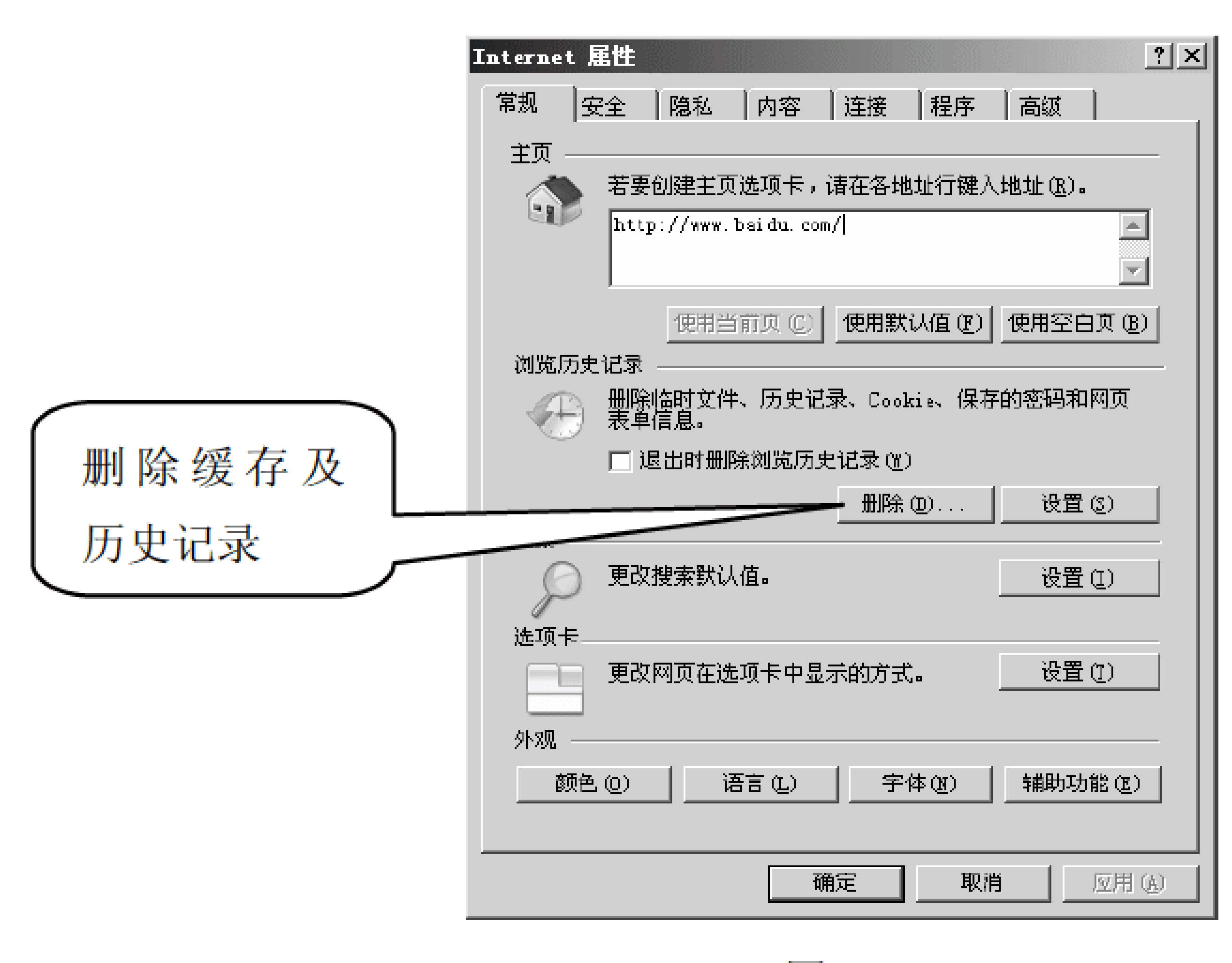


图 9-1

02 弹出【删除浏览的历史记录】对话框，选择需要删除的选项的复选框，单击【删除】按钮，如图 9-2 所示。

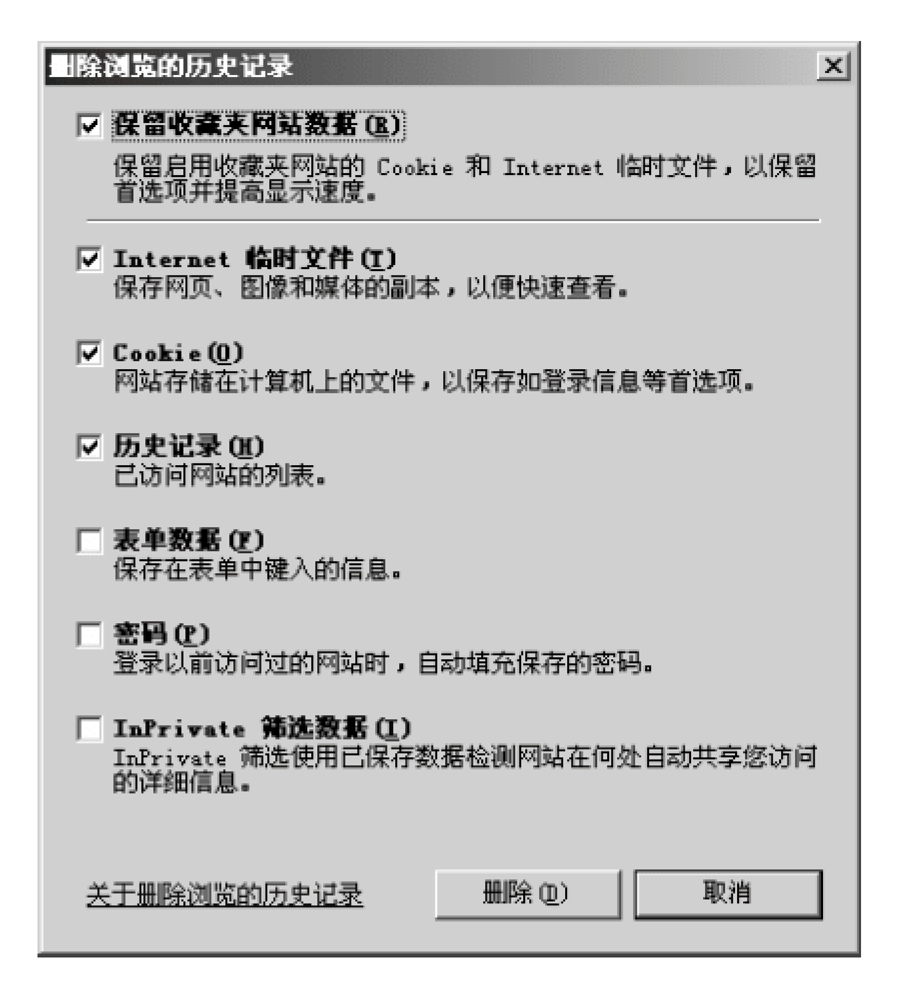


图 9-2

2. 网络钓鱼攻击

近些年钓鱼网站频繁出现，其中比较多的是网购类的网站。有些黑客使用淘宝网网页模板制造可以窃取用户支付宝或银行卡账户信息的钓鱼网站，使不少用户财产受损。

诸如此类的钓鱼攻击手段还有很多，作为用户需要注意，通过网络进行消费时，一定要确认其网站是官方网站，比如淘宝网的网址中一定会有“taobao.com”字样，即便是官方网站也要尽量搜集信息确定网站信息真伪，不要想着天上会掉馅饼，没有白捡的便宜。

3. 漏洞攻击

无论是操作系统、硬件设备、还是软件程序都有可能存在漏洞，这些漏洞很有可能被攻击者利用。虽然有些用户为了安全会进行补丁更新，但是网络攻击者总是会在漏洞出现后，网络用户未更新补丁前的时差范围内开始自己的行动。这就需要有完善的漏洞扫描、补丁更新计划做保证。

4. 病毒泛滥

病毒是用户网络最常见的危害之一，随着其数量、类型越来越多，造成的危害也在逐步增加。每一次病毒的泛滥都会对整个互联网用户造成巨大的损失。

5. 僵尸网络

网络攻击者通常会向互联网散布大量的木马程序，一旦用户被感染，就会被攻击者操控、查看个人信息。这种现象很多，从目前整个互联网来看，很多用户和企业的网络都存在被人植入控制程序的现象。被控的僵尸网络在整个网络中的比重很大，所以这对整个互联网的危害也很大。

6. 无线网络安全威胁

目前，无线网络越来越普及。虽然无线网络使用很方便，但是整个无线网络信号一直处于暴露状态，很容易被攻击者攻入，窃取网络信息。只要攻击者能够进入企业或家庭个人的无线网络区

域，就可以接入无线网。即使现在大部分无线网络都使用了无线认证加密技术，但是碍于它的特性，比之有线网络的安全性还有很大的差距。

9.2 网络攻击的入口

端口是电脑与外界网络连接的一扇门，在某种程度上，端口掌握着网络连接大权，同时也是网络攻击的入口。

9.2.1 端口的分类

在 Windows 系统端口的分配中，按照端口号可以将端口划分为公认端口、注册端口、动态端口三种。下面将分别介绍每一种端口。

1. 公认端口

公认端口的范围是 0~1023，它们紧密绑定于一些服务。通常这些端口明确表明了某种服务的协议，例如：80 端口代表 HTTP 通讯。

2. 注册端口

注册端口的范围是 1024~49151。注册端口松散地绑定于一些服务，目前许多服务绑定于端口，许多系统动态处理端口都是从 1024 左右开始的。

3. 动态端口

动态端口的范围是 49152~65535。但是实际上，计算机通常从 1024 起分配动态端口。不过也有例外：如 SUN 的 RPC 端口从 32768 开始。

9.2.2 开启和关闭端口

为了保护计算机，可以将危险的端口关闭，同样也可以开启一些有用的端口。开启与关闭端口有通过“TCP/IP 筛选”和禁用或开启服务两种方法。

1. 关闭端口

如果哪个端口出现漏洞就关闭哪个端口，这样是不能保证系统安全的，正确的方法应该是先了解清楚自己需要开放哪些端口，然后把自己不需要的端口统统关闭掉，这样才能保证系统的安全性。

下面介绍如何通过“TCP/IP 筛选”和禁用服务两种方法关闭端口，具体操作步骤如下。

01 在电脑桌面上，在【网上邻居】图标上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单命令，即可打开【网络连接】窗口，如图 9-3 所示。



图 9-3

02 在【本地连接】图标上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单命令，即可打开【本地连接 状态】对话框，如图 9-4 所示。



图 9-4

03 单击【属性】按钮，即可打开【本地连接属性】对话框。在【此连接使用下列项目】列表中选择【Internet 协议（TCP/IP）】选项，如图 9-5 所示。



图 9-5

04 单击【属性】按钮，即可打开【Internet 协议（TCP/IP）属性】对话框，如图 9-6 所示。

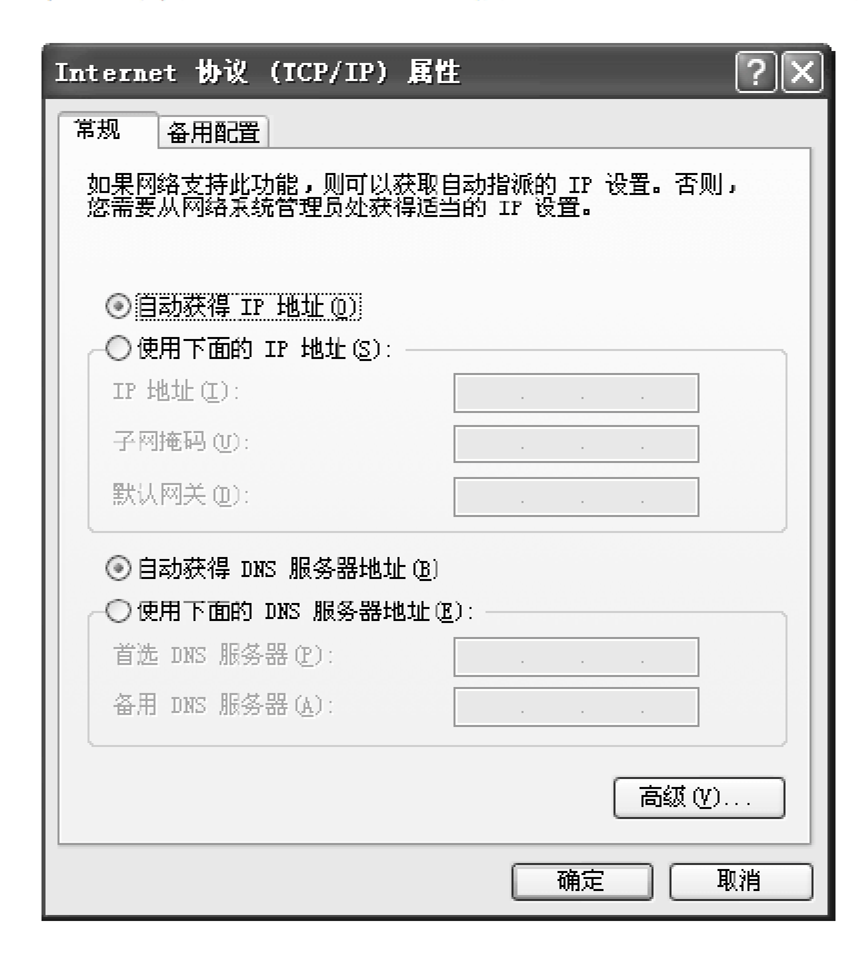


图 9-6

05 单击【高级】按钮，即可打开【高级 TCP/IP 设置】对话框，并单击【选项】选项卡，如图 9-7 所示。



图 9-7

06 在【可选设置】栏目中选择【TCP/IP 筛选】选项，然后单击【属性】按钮，即可打开【TCP/IP 筛选】对话框，如图 9-8 所示。

TCP/IP 筛选
启用 TCP/IP 筛选(所有适配器)(E)
全部允许(P)　全部允许(M)　全部允许(I)
只允许(Y)　只允许(N)　只允许(L)
TCP 端口　UDP 端口　IP 协议
添加...　添加...　添加...
删除(R)　删除(O)　删除(V)
确定　取消

图 9-8

07 选择【启动 TCP/IP 筛选（所有适配器）】复选项，并在【TCP 端口】栏目中选择【只允许】单选按钮，然后单击【添加】按钮，即可打开【添加筛选器】对话框，如图 9-9 所示。



图 9-9

08 在【TCP 端口】文本框中输入“80”后，单击【确定】按钮，即可在【添加筛选器】对话框中看到添加的端口号。按照同样的方法添加允许开启的端口，这样就把那些危险端口关闭了，如图 9-10 所示。

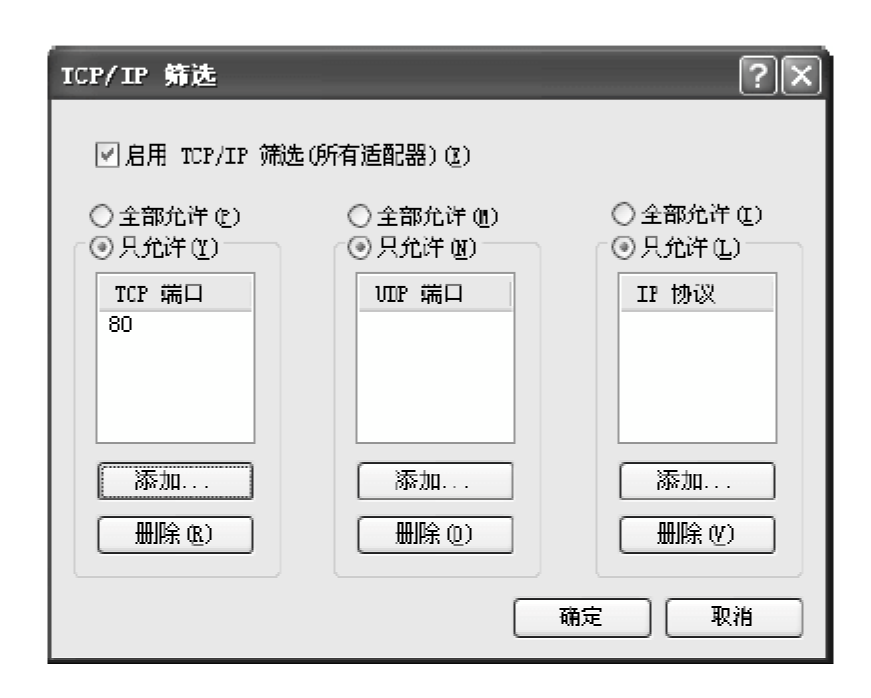


图 9-10

09 由于计算机中的服务是与端口相对应的，所以也可以通过禁用相应的服务来关闭端口。选择【开始】➢【控制面板】菜单命令，即可打开【控制面板】窗口，如图 9-11 所示。

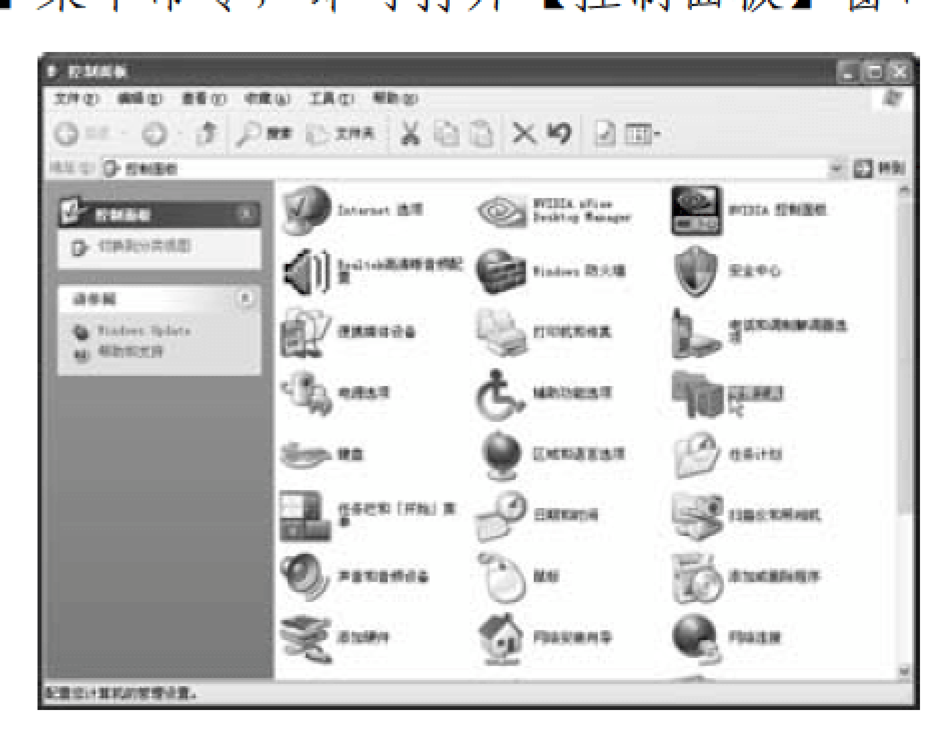


图 9-11

10 单击【管理工具】图标按钮，即可打开【管理工具】窗口，如图 9-12 所示。



图 9-12

11 单击【服务】图标按钮，即可打开【服务】窗口。在其中可以看到本地计算机中所有服务及其所处的状态，如图 9-13 所示。

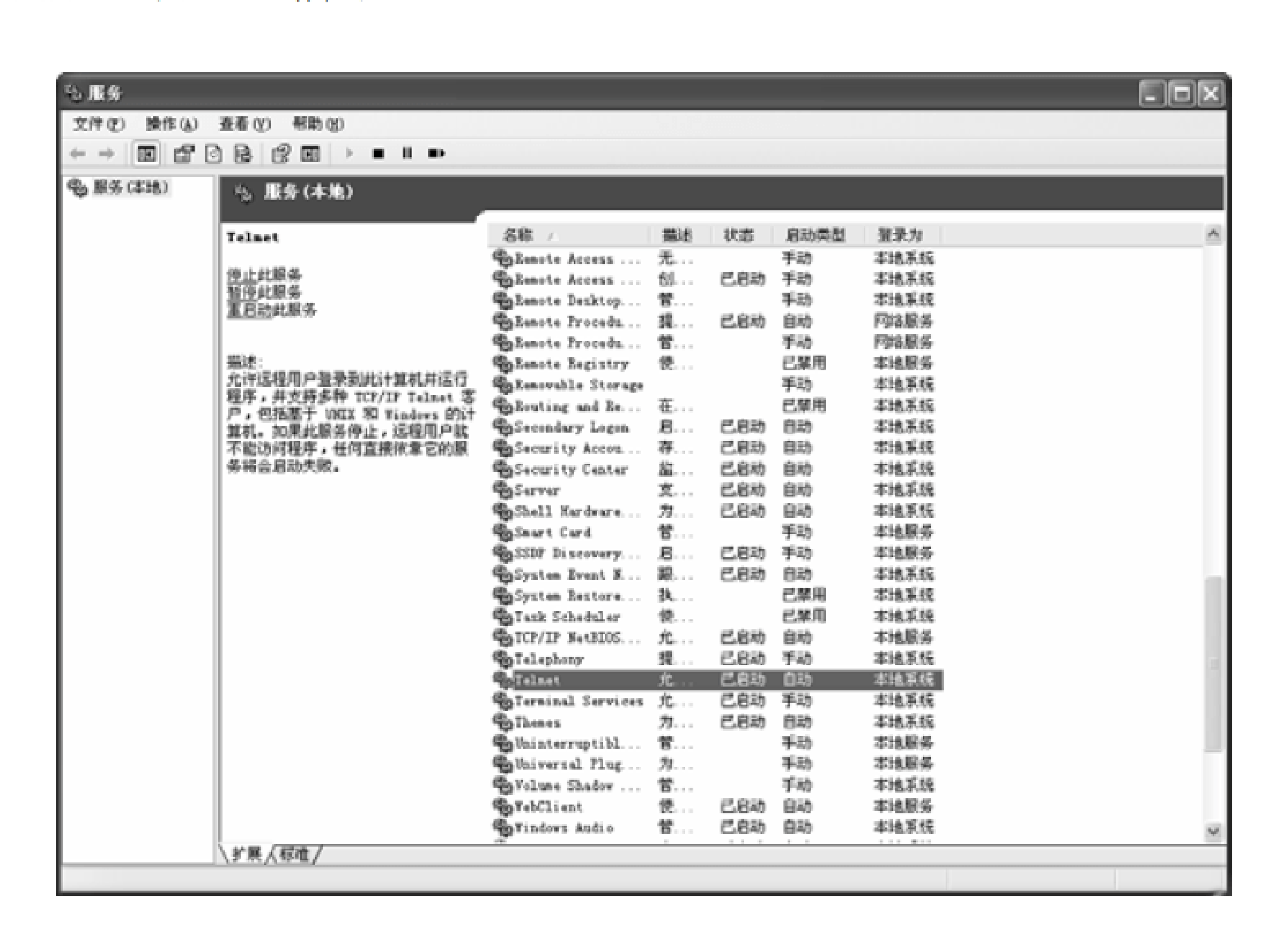


图 9-13

12 在要停用的服务上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，即可打开【Telnet 的属性（本地计算机）】对话框，如图 9-14 所示。



图 9-14

13 单击【停止】按钮，即可进行禁用该项服务的操作，待操作完成后，在【Telnet 的属性】对话框中，即可看到 Telnet 服务的【服务状态】已经变为【已停止】，如图 9-15 所示。



图 9-15

14 单击【确定】按钮，返回到【服务】窗口中，此时即可发现 Telnet 服务的【启用类型】被设置为【已禁用】，这样就可以成功关闭 Telnet 服务对应的端口了，如图 9-16 所示。



图 9-16

2．开启端口

与关闭端口的方法类似，开启端口也有两种方式，通过【TCP/IP 筛选】方式开启端口的方法只需输入要开启的端口号即可实现。这里介绍通过启动服务来开启端口的具体操作步骤。

01 以上面停止的 Telnet 为例，如图 9-17 所示，在【Telnet 的属性】对话框中的【启动类型】下拉列表中选择【自动】命令。单击【应用】按钮，即可激活【启动】按钮。



图 9-17

02 单击【启动】按钮，进行启动该项服务的操作，待操作完成后，在【Telnet 的属性】对话框，即可看到 Telnet 服务的【服务状态】已经变为【已启动】，如图 9-18 所示。

图 9-18

03 单击【确定】按钮，返回到【服务】窗口中，此时即可发现 Telnet 服务的【启用类型】被设置为【已启动】。这样就可以成功关闭 Telnet 服务对应的端口，如图 9-19 所示。

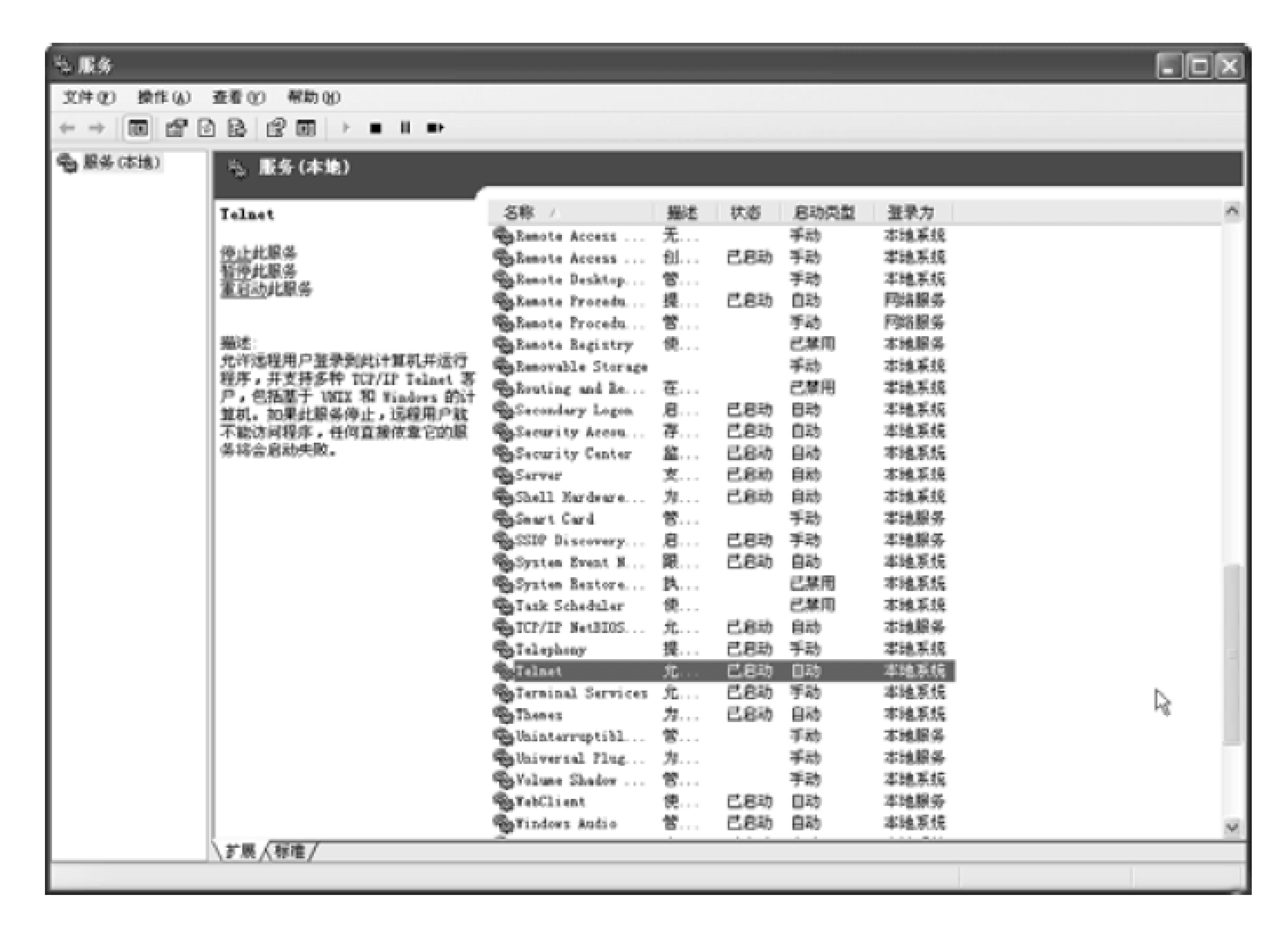


图 9-19

9.3 寻找木马的藏身之处——进程

进程是在计算机系统中运行的一个应用程序，进程是木马程序主要的藏身地，在本节将介绍有关系统进程的基本知识以及一些基本的操作。

9.3.1 认识系统进程

进程是在系统中正在运行的一个应用程序；而线程是系统分配处理器时间资源的基本单元，或者说是进程之内独立执行的一个单元。对于 Windows 操作系统而言，其调度单元是线程。一个进程至少包括一个线程，通常将该线程称为主线程。一个进程从主线程的执行开始进而创建一个或多个附加线程，即基于多线程的多任务。

进程是系统运行的基本条件，有了这些进程，系统才可以正常运行。Windows XP 中正常的系统进程如下。

1. svchost.exe

进程文件：svchost 或者 svchost.exe

进程名称：microsoft service host process

作用：svchost.exe 是一个属于微软 Windows 操作系统的系统程序，用于执行 dll 文件。这个程序对系统的正常运行是非常重要的。

2. iexplore.exe

进程文件：iexplore 或者 iexplore.exe

进程名称：microsoft internet explorer

作用：iexplore.exe 是 Microsoft Internet Explorer 的主程序。这个微软 Windows 应用程序让用

户实现网上冲浪和访问本地 internet 网络。

3. rundll32.exe

进程文件：rundll32 或者 rundll32.exe

进程名称：microsoft rundll32

作用：rundll32.exe 用于在内存中运行 dll 文件，它们会在应用程序中被使用。这个程序对系统的正常运行是非常重要的。

4. ctfmon.exe

名称：alternative user input services

作用：ctfmon.exe 是 Microsoft Office 产品套装的一部分。它可以选择用户文字输入程序。

5. winlogon.exe

进程文件：winlogon 或者 winlogon.exe

进程名称：microsoft windows logon process

作用：winlogon.exe 是 Windows 域登陆管理器。它用于处理登录和退出系统过程。

6. wdfmgr.exe

进程文件：wdfmgr 或者 wdfmgr.exe

进程名称：windows driver foundation manager

作用：wdfmgr.exe 是微软 Microsoft Windows Media Player 10 播放器的相关程序。该进程用于减少兼容性问题。

7. alg.exe

进程文件：alg 或者 alg.exe

进程名称：application layer gateway service

作用：alg.exe 是微软 Windows 操作系统自带的程序。它用于处理微软 windows 网络连接共享和网络连接防火墙。

8. smss.exe

进程文件：smss 或者 smss.exe

进程名称：session manager subsystem

作用：smss.exe 是微软 Windows 操作系统的一部分。该进程调用对话管理子系统和负责操作系统的对话。

9. explorer.exe

进程文件：explorer 或者 explorer.exe

进程名称：microsoft windows explorer

作用：explorer.exe 是 Windows 程序管理器或者 Windows 资源管理器，它用于管理 Windows 图形壳，包括开始菜单、任务栏、桌面和文件管理。删除该程序会导致 Windows 图形界面无法适用。

10. csrss.exe

进程文件：csrss 或者 csrss.exe

进程名称：microsoft client/server runtime server subsystem

作用：csrss.exe 是微软客户端/服务端运行时子系统。该进程管理 Windows 图形任务。

11. lsass.exe

进程文件：lsass 或者 lsass.exe

进程名称：local security authority service

作用：lsass.exe 是一个关于微软安全机制的系统进程，主要处理一些特殊的安全机制和登录策略。

12. timplatform.exe

timplatform.exe 是 QQ 和 Tencent Messenger 共同使用的外部应用开发接口管理程序，属于 QQ 不可或缺的底层核心模块。如果删除该程序，QQ 将丧失与周边功能模块以及外部应用程序相互调用的功能。

9.3.2　查看、新建和关闭系统进程

在 Windows XP 系统中，可以在【Windows 任务管理器】窗口中查看、新建和关闭系统进程。下面介绍查看、新建和关闭系统进程的具体操作步骤。

01 在 Windows XP 系统中，按下【Ctrl+Del+Alt】组合键，即可打开【Windows 任务管理器】窗口。在其中即可看到当前系统正在运行的进程，如图 9-20 所示。



图 9-20

02 选择【文件】➢【新建任务】菜单命令，即可打开【创建新任务】对话框。在【打开】文本框中输入新建的进程名称，单击【确定】按钮即可创建一个新的进程，如图 9-21 所示。



图 9-21

03 可以在【Windows 任务管理器】窗口设置显示进程的各个属性。在【Windows 任务管理器】窗口中选择【查看】➢【选择列】命令，即可打开【选择列】对话框，如图 9-22 所示。

选择列
请选择“任务管理器”进程页上将显示的列。
映像名称(I)
PID (进程标识符)(P)
CPU 使用(C)
CPU 时间(E)
内存使用(M)
内存使用增量(D)
内存使用高峰值(K)
页面错误(F)
USER 对象(U)
I/O 读取
I/O 读取字节
会话 ID(S)
用户名(N)
页面错误增量(A)
虚拟内存大小(V)
页面缓冲池(G)
非页面缓冲池(O)
基本优先级(R)
句柄计数(H)
线程计数(T)
GDI 对象(J)
I/O 写入
I/O 写入字节
I/O 其他
I/O 其他字节
确定
取消

图 9-22

04 选择【PID（进程标识符）】复选项，单击【确定】按钮即可在【Windows 任务管理器】窗口看到各个进程对应的 PID 号，如图 9-23 所示。



图 9-23

05 在【Windows 任务管理器】窗口中选中要结束的进程，单击【结束进程】按钮，即可关闭该进程，如图 9-24 所示。



图 9-24

06 如果删除的是系统进程，则会弹出【任务管理器警告】对话框。此时应该单击【否】按钮取消删除进程，如图 9-25 所示。

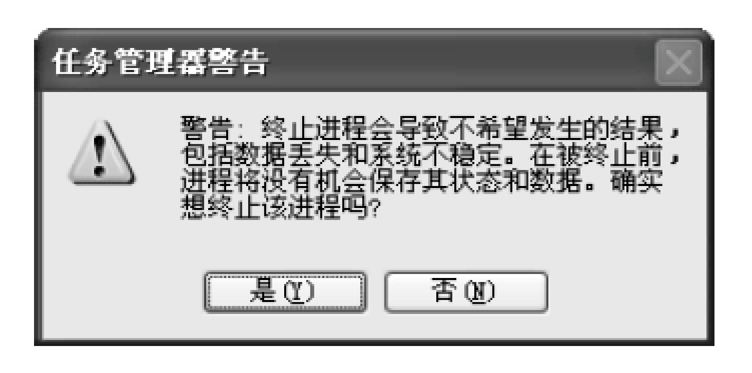


图 9-25

9.3.3 查看进程起始程序

可以通过查看进程的起始程序，来判断哪些进程是恶意进程。下面来介绍查看进程起始程序的具体操作步骤。

01 在【命令提示符】窗口中输入查看进程 svchost 进程的起始程序的“Netstat –abnov”命令，如图 9-26 所示。

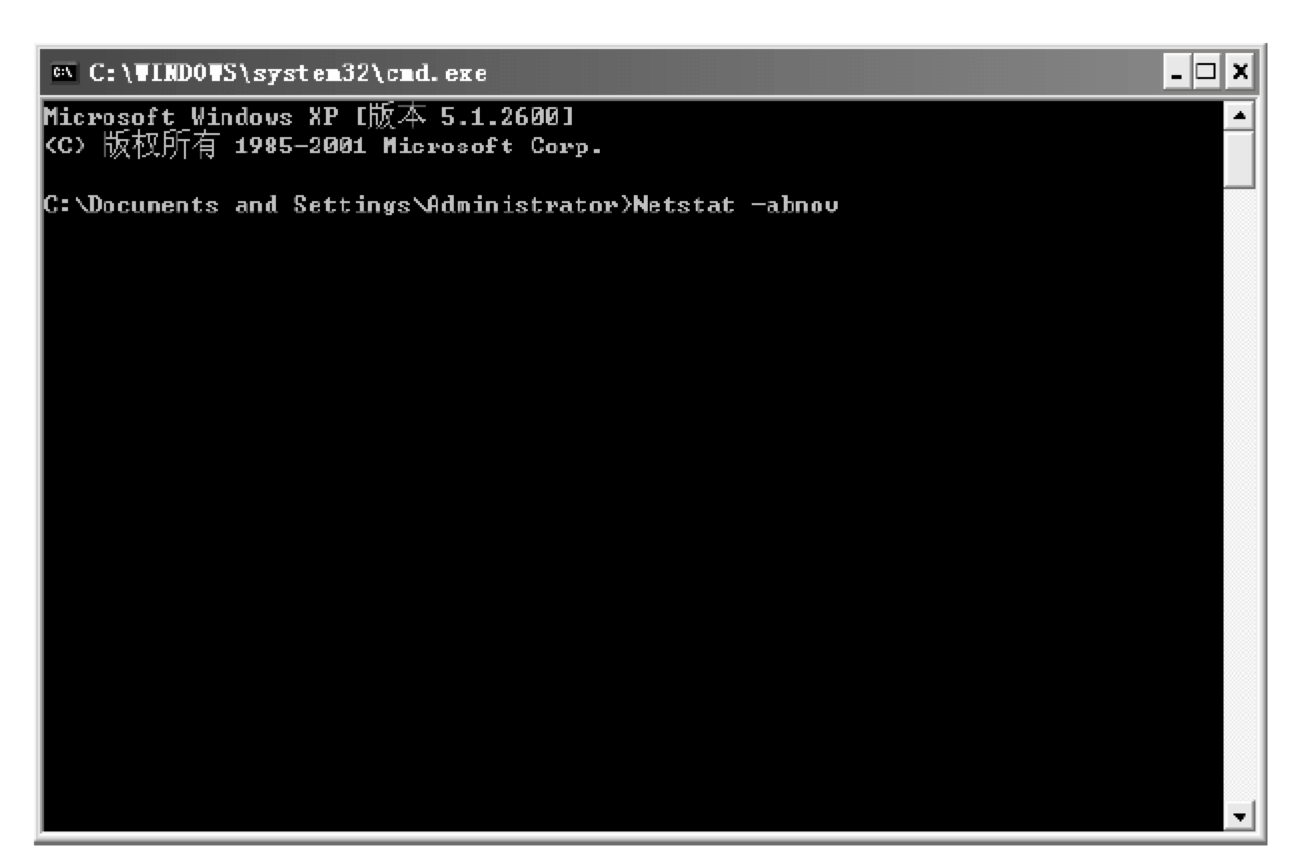


图 9-26

02 按下【回车键】，即可在反馈的信息中查看每个进程的起始程序或文件列表，如图 9-27 所示，这样就可以根据相关的知识来判断是否为病毒或木马发起的程序。

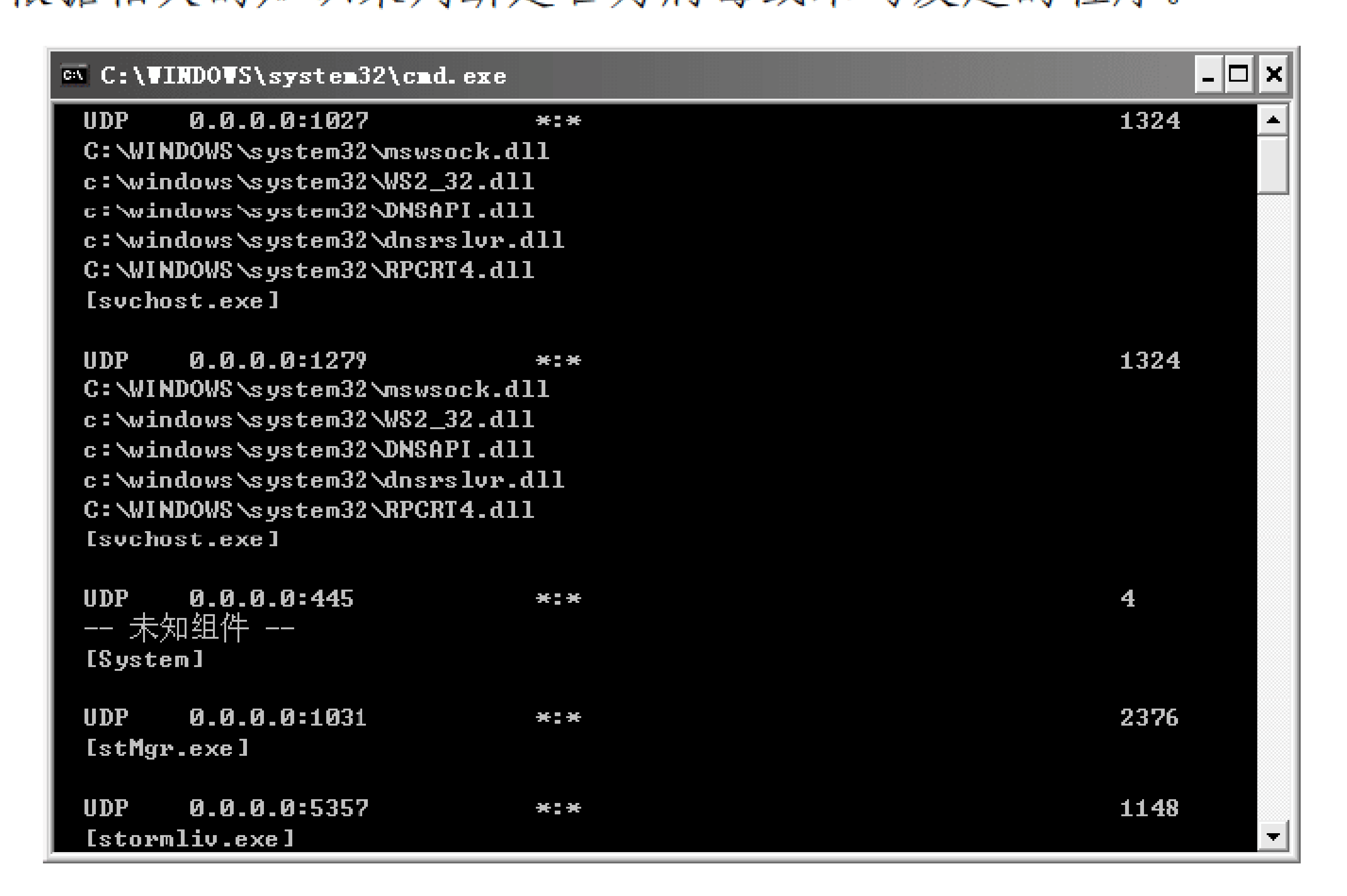


图 9-27

9.4 网络安全防护策略

实施网络安全保护时，可以将网络安全分为多个部分，分别实施。主要有：物理安全防护、主机安全防护、应用程序和服务安全防护、网络结构安全防护。下面分别做介绍。

9.4.1 物理安全防护

物理设备是整个网络的基础，所谓物理安全防护就是保护这些计算机、路由器、交换机、网线等物理设施的安全。

通常保护物理安全可以从以下几点考虑。

1. 自然灾害

自然灾害一般认为是无法控制的一类安全威胁，常见的自然灾害有：地震、水灾、火灾等。对付这些自然灾害只能采取防患于未然的方式，可以建设安全的机房建筑，增强其抗震、防火、防水能力。

2. 电源故障

网络的运行需要电源做支持，但是难免会出现电网故障的现象，为了保证网络不会受电源的影响，应当增加 UPS 不间断电源。

3. 人为操作失误或错误

设备安装、使用过程中，很容易出现操作错误，特别是计算机。解决这部分故障，需要操作者具有良好的技术水平和工作态度。

4. 设备被盗、被毁

这是比较恶意的行为，特别是在室外安放的设备，比如运营商在外分布的接入点。这需要配备标准机柜，并在重要设备附近增加监控设备。

5. 电磁干扰

一般在高压线路设备附近会产生强电磁场，产生的电磁信号会严重影响网络弱电系统的信号传输，一般建议强电和弱电分离安装，对于有环境限制的要确保在弱电系统外有屏蔽层。

6. 线路截获

很多网络线路是暴露在外的，攻击者如果可以接触到线缆就可以实现信息截获。所以要确保线路隐蔽，或不可触及。

7. 高可用性的硬件

硬件设备自身的稳定性也是很重要的，在进行设备采购时一定要确保设备性能及其可用性。

8. 冗余备份技术

网络一旦出现故障，可能整个网络的业务都无法正常使用，为了网络的不间断使用，可以使用双机热备、以太网信道、系统群集等技术实现冗余备份。即使出了故障也可以确保网络正常的运行。

9.4.2 主机安全防护

主机安全防护主要针对的是网络设备、服务器、主机的操作系统，需要确保这些系统安全可靠。除了网络设备自带的系统镜像外，使用最多的操作系统是 Microsoft 的 Windows server 2003、Windows server 2008、Windows XP、Windows 7，Linux 的红旗、红帽、CentOS，还有 UNIX 和其他各厂商自己的系统。其中，Windows 系列的服务器操作系统中小企业使用比较多，但其安全性却是最弱，相比之下，Linux 系列的操作系统要安全很多。结合业务需求，企业应尽量选择安全级别高的系统。

当然，这些系统没有一个是绝对安全的，大都存在有漏洞和兼容性问题。在使用时需要实时更新补丁，同时要规范使用方法，如安全登录系统，不对系统做错误的系统配置等。

通常可以使用系统性能分析、漏洞扫描和单机防病毒程序确保主机安全。

9.4.3 应用程序和服务安全防护

各类应用软件程序和服务器配置都有可能存在安全问题，比如 Office 办公软件程序安全漏洞、WEB 服务器安全问题。随着应用程序不断的更新，所产生的安全问题也会动态的更新。不过总的来说，以 Internet 为基础的应用程序安全问题为主。

WEB 服务器、E-mail 服务器、DNS 服务器都是比较常见的应用服务，通常会采取比较的方式来实现，比如使用 apache+tomcat 搭建 WEB 服务器、使用 sendmail 搭建 E-mail 服务器等。

9.4.4　网络结构安全防护

网络拓扑结构的设计对于网络安全影响很大。比如服务器和员工客户机如果连接在同一个局域网交换机下，且没有做任何安全隔离，就很容易威胁服务器的安全。

网络拓扑连接即便看着很合理也不一定就能确保安全，还要配置合理的网络流量控制与网段隔离。而且不同节点的性能也要满足要求，比如核心设备的性能需要满足所有分支网段信息转发的需求。

信息在网络中传输，网络结构的设计还需要满足对这些信息的加密、认证保护功能。比如使用安全的通信协议，高级别的加密手段等。

9.5　专家答疑

（1）有哪些技术可以用于实现网络安全？

答：加密技术、认证技术、系统安全分析、防火墙、漏洞扫面与安全风险评估、IDS 入侵检测、恶意代码防护、审计与因特网内容分析、VPN。

（2）防火墙和 IDS 入侵检测系统有什么差异？

答：防火墙主要用于防护企业外部网络攻击，具有很好的隔离内网功能。企业防火墙可以作为内网的安全网关，确保内网免受外网非法用户的入侵。防火墙可以通过服务访问规则、验证技术、包过滤和应用网关四部分功能，使流入流出的所有信息被监控，所有具有安全隐患的流量都可以被拒绝转发。

入侵检测系统是一种主动保护自己免受攻击的网络安全系统，是防火墙技术的合理补充，入侵检测系统能够帮助系统对付网络的攻击，这就在一定程度上提高了系统管理员的安全管理能力，包括安全审计、监视、攻击识别和响应等，也提高了信息安全基础结构的完整性。

通过使用入侵检测软件，对计算机网络或计算机系统中的若干关键点收集信息，并对这些信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。

第 10 章　中小型企业网络安全项目分析

对于大部分企业来说，最担心的就是网络安全问题。这主要是受近些年来频繁的网络安全事件影响，同时随着信息产业的飞速发展，信息的重要性也增强了企业对安全的重视。

各个企业纷纷将目光投向网络安全加固，各种最新网络安全产品被一一部署，但是网络攻击者的手段很多，即使是再好的安全设备，没有配置好也只能做个摆设。所以企业实施网络安全加固时考虑的不应该只是设备有多新，而应该是如何更全面的保证网络安全。

本章节将结合一个企业网络环境，对其进行网络安全分析及网络安全方案设计。

10.1　项目介绍

首先来了解一下企业的概况及网络现状。

1. 公司简介

某 IT 企业成立于 2004 年，有 200~300 名员工，主要从事软件开发及电子产品生产。在这七年时间里，企业有了飞速的发展，除了北京总部外，在全国各地还有多家子公司。在北京总部，员工数量比较多，除此之外还有一部分员工需要经常出差移动办公。在各个子公司，员工数量相对较少，主要进行产品加工及分销工作。

2. 网络现状

网络现状可以总结为以下几点。

（1）全部使用 Cisco 产品，并使用了三层交换机。

（2）总公司与子公司业务量比较少，通过 QQ 等互联网工具进行通信。

（3）企业有一部分移动及家庭办公员工。

（4）在总公司内配置了供员工访问的 FTP、WEB、数据库等服务器，。

（5）为了宣传企业形象，在公共网络 IDC 机房托管一台服务器，用于发布企业官方网站、OA 及邮件系统。

（6）企业总部员工使用全交换网络互联，为了减少广播使用了 VLAN 隔离。

（7）企业总部出口采用 10M 光纤，子公司一般采用 4M 宽带。

3. 网络拓扑

根据网络环境绘制如图 10-1 所示网络拓扑图。

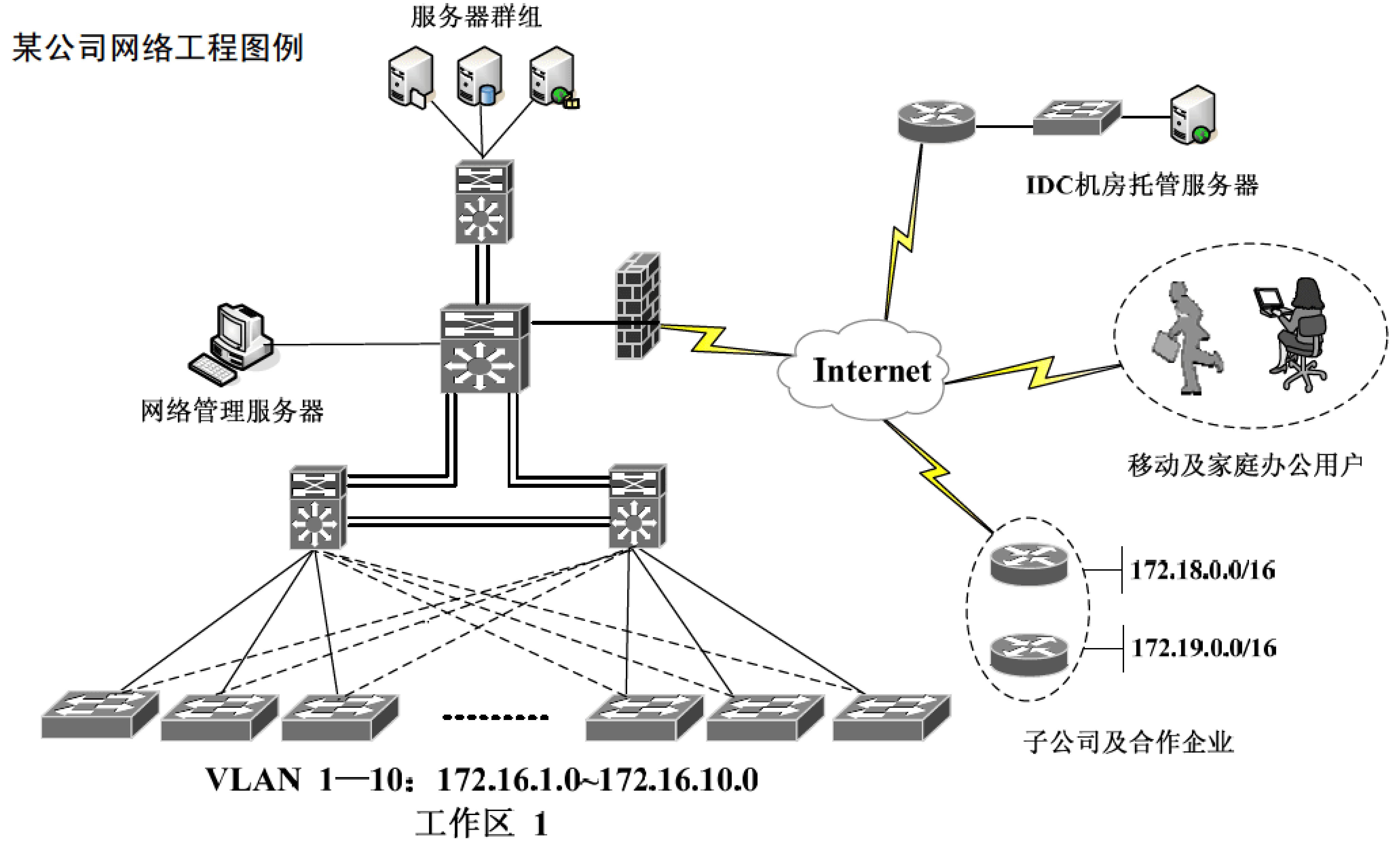


图 10-1

4. 网络安全现状

企业网络环境已成规模，但是网络安全隐患很多，目前存在的网络安全问题有以下几点。

（1）企业内网服务器安全性较低，没有实施安全加固。

（2）网络设备未作安全配置，存在安全隐患。

（3）子公司和移动及家庭办公员工需要访问企业网络资源时没有安全保障，信息容易被窃取。

（4）企业对外发布服务器放在 IDC 机房托管，不便于安全管理。

（5）企业网络员工比较多，网络攻击及病毒威胁频繁。

结合以上网络安全问题，该企业必须做出及时的安全加固调整。

10.2　需求分析

结合企业网络安全现状，做出如下分析。

1. 服务器安全级别低，易频繁受到攻击

企业服务器分为两部分，一个是内网服务器，一个是外网服务器。该企业内部服务器通过一台交换机连接到核心三层交换机上，与内部员工处于同一个交换网络，虽说有 VLAN 隔离，但是在核心交换机上没有做好访问控制，员工客户机依然会威胁到内网服务器安全。而外网服务器在

IDC 机房托管，和其他众多服务器放置在一起，虽说在 IDC 机房出口有网络安全设备，但是只要有一台服务器受到威胁，其他 IDC 机房的服务器都会有安全隐患，同时企业重要数据放置在 IDC 机房服务器中很容易被人恶意拷贝。

对于服务器来说，最主要的威胁就是网络攻击和病毒，目前网络环境中只有一个防火墙具有较强的安全隔离作用，无法达到网络安全的要求。

解决办法：首先需要对所有服务器实施反病毒系统，同时要在服务器上配置基于主机的 IDS 入侵检测系统。其次要做到对外部网络攻击实时监控，除了上面的基于主机 IDS 外，还要在网络中加入基于网络的 IDS 入侵检测系统。再次，为了保证企业重要数据的安全，在 IDC 机房服务器只放置必要的对外发布服务即可，其他需要对外发布的服务器放置在出口防火墙设备的 DMZ（隔离区）中。最后，为了防止内网员工主机威胁服务器，可以在关键网络设备上配置访问控制策略。

2. 网络设备存在安全隐患

网络设备自出厂之后有很多的默认配置，这些默认配置很有可能被网络攻击者利用，同时网络设备自身也存在一些漏洞。现在大部分的网络都是交换网络，一旦有一个网络设备被攻击，很有可能将威胁延伸到其他设备及其网络。

解决办法：尽量不采用设备的默认配置，并及时更新网络设备的系统，能够添加认证、口令的位置尽量添加。

3. 子公司和移动及家庭办公员工访问企业网络没有安全保障

子公司和总公司虽然业务量很少，但是这些业务信息如果被窃取也可能造成不小的损失，同时部分员工需要在外或家中移动办公，办公中难免要访问企业内的服务器或网络，这部分信息也需要被安全保护。

解决办法：对移动及家庭办公用户可以采用远程访问 VPN 技术连接，而和子公司之间传输的信息量相对较多一些，也需要长期保持联系，则可以采用 IPSec VPN 技术。

4. 企业员工主机频繁遭受网络攻击及病毒威胁

企业员工比较多，一旦有一台感染了病毒或木马，又或者遭到了网络攻击，就很有可能威胁到全网安全。病毒或木马会迅速扩散到整个网络，单靠个人防火墙及杀毒软件根本不可能彻底清除，同时员工的计算机水平差异很大，很多员工没有能力进行安全防护。

解决办法：单靠员工个人根本不行，所以需要在网络攻击到达员工主机之前被尽量的屏蔽掉，对于没能屏蔽掉的网络威胁，需要进行控制，这主要可以通过两种手段解决：一方面在网络入口位置架设基于网络的入侵检测系统、防火墙系统；另一方面在整个网络运行企业版网络反病毒系统，通过网络管理员对全网所有主机进行病毒监控和查杀。

通过以上分析，可以对网络实施以下改造。

（1）对网络内所有主机、服务器安装企业反病毒客户端，能实现通过企业反病毒控制端进行全网病毒监控、扫描、查杀。

（2）对企业内所有服务器架设基于主机的入侵检测系统，同时在出口防火墙内网接口下连接基于网络的入侵检测系统。

（3）将 IDC 机房托管服务器上的企业重要数据信息放置到企业内部发布，在出口防火墙配置 DMZ 区，用于发布这些重要数据业务服务。

（4）尽量关闭所有服务器、网络设备的安全漏洞，通过访问控制尽量限制无意义或有安全威胁的流量。

（5）对在外办公及子公司配置 VPN，主要采用 IPSec VPN 和远程访问 VPN。

结合以上改造内容，可对企业网络拓扑图进行调整，调整后的拓扑图如图 10-2 所示。

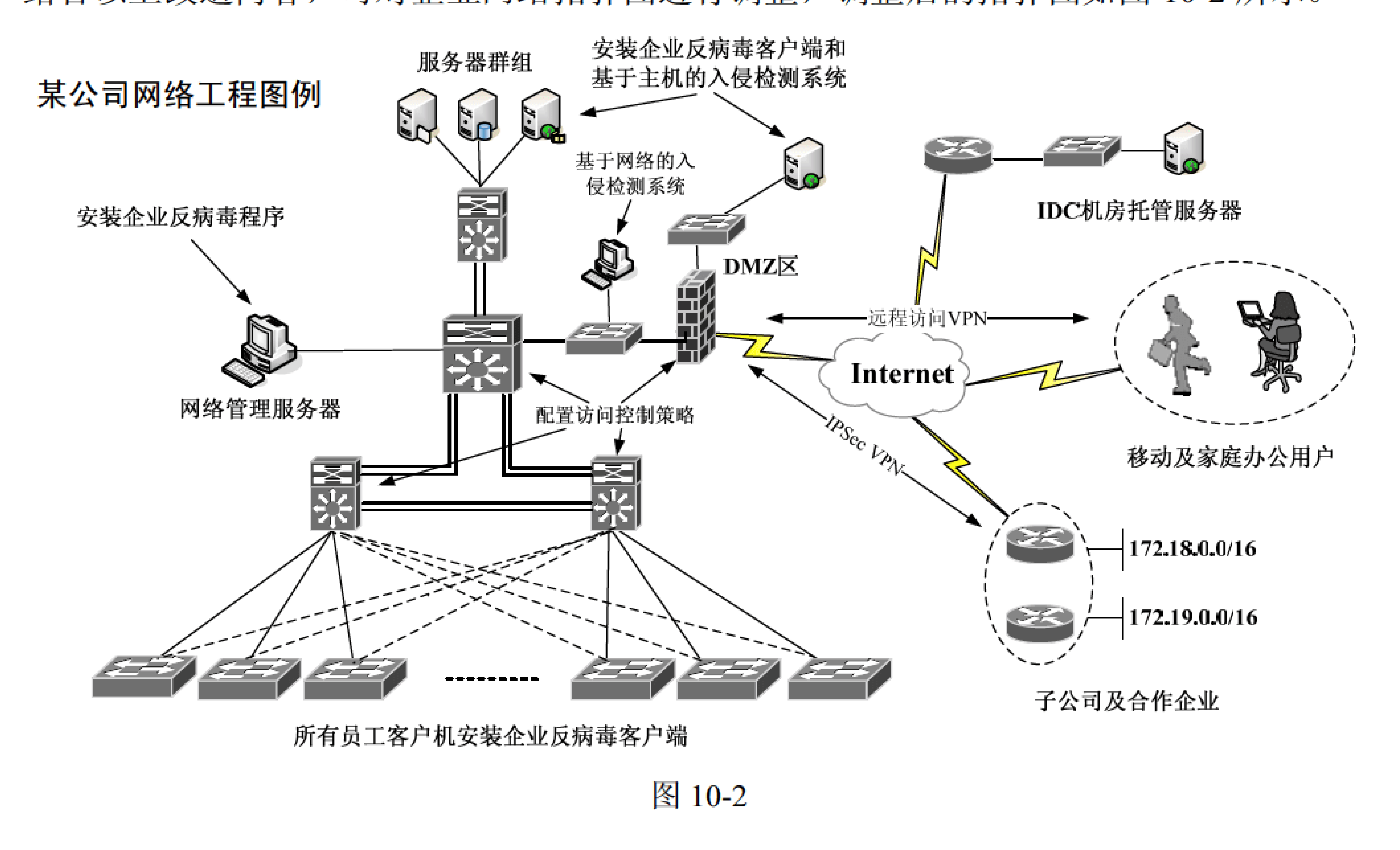


图 10-2

10.3 项目实施流程

整个网络可以分为总公司内网、内网网络出口和总公司外网三部分。整个网络安全改造方案的实施，也可以从这三个部分分别完成。结合上文的需求分析，网络安全改造方案实施步骤如下。

10.3.1 服务器设备安全

首先要解决的是企业服务器、客户机和网络设备的安全威胁问题，解决这几方面的改造内容需要从以下四点来分别实现。具体内容介绍如下。

1. Windows 服务器安全

本方案中服务器使用的基本是 Windows 服务器，Windows 服务器本身的安全漏洞比较多，所以要对所有服务器进行补丁、漏洞更新。另外每一台服务器所发布的服务都比较单一，比如 WEB 服务器只需要发布 HTTP 的 80 端口，同时为了方便管理远程桌面程序的 3389 端口或其他远程服务器管理程序的端口，也需要被允许访问。这样一来，只需要允许这些必要端口被访问，其他端口尽量关闭就可以减少网络威胁了。进行操作时可以通过组策略进行配置。

在配置时为了防止必要流量被屏蔽，可以只屏蔽已知的有安全威胁的端口，常见的有安全威胁的端口有 TCP 的 135、139、445、593、1025、3389 端口和 UDP 的 135、137、138、445 端口，除此之外还有一些流行病毒的后门端口，如 TCP 的 2745、3127、6129 端口。

除了以上配置之外，还可以在服务器上配置入侵检测系统，来防护其安全。Windows 服务器本身的不安全因素很多，应对种类繁多的网络攻击手段很难做到绝对安全。而入侵检测系统是专门监测网络入侵的程序，对于发现、屏蔽网络攻击有几大优势。

入侵检测系统有两类，分别是：基于主机的入侵检测系统和基于网络的入侵检测系统。其中基于主机的入侵检测系统主要用于防护单个服务器的安全，可以按照图 10-3 实施改造。

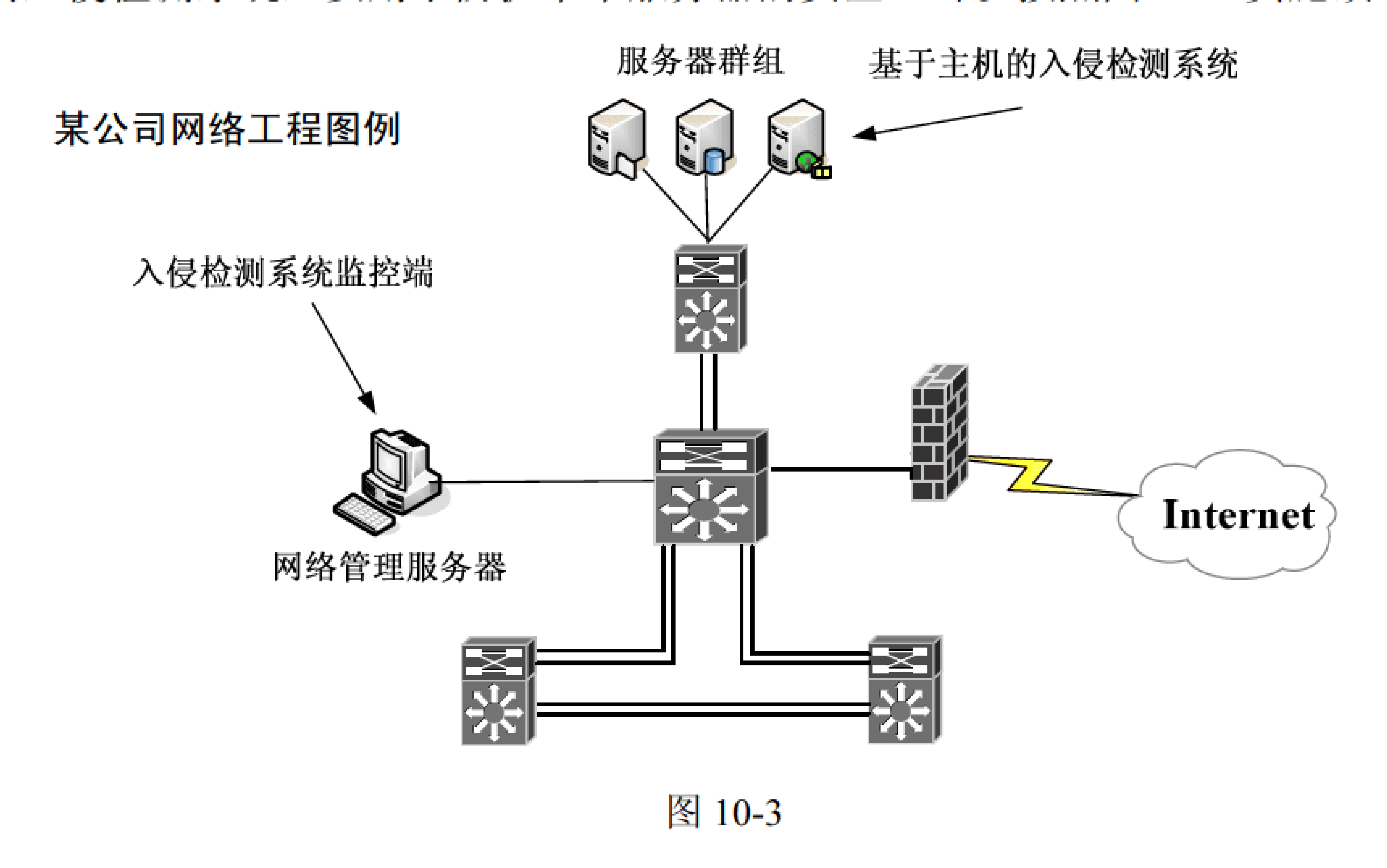


图 10-3

2. 网络设备安全

网络设备作为网络的重要组成部分，它们的安全性显得尤为的重要。网络设备的安全问题主要在于默认配置及漏洞。很多设备都配置了默认口令，开启了很多默认服务，这些信息很容易被攻击者利用。同时网络设备运行的一些协议也存在着漏洞，比如 SNMP 协议、CDP 协议。所以网络设备配置后首先要将其所有可能被利用的默认配置修改掉，并将没有必要的服务关闭，尽量降低被攻击的可能性。

网络设备作为网络中大量数据的必经之地，如果能在网络攻击经过之前就将其屏蔽掉，必然会减少很多网络威胁，这主要依靠网络设备的访问控制功能。通过访问控制列表可以禁止所有不需要或有威胁的流量转发。

3. 无线安全

本案例中没有配置无线网络，但是大部分企业已经存在无线网络了，而且大都是使用的出口无线路由器的无线功能。本案例可以在防火墙外端加入无线路由器，或者在交换机下连接无线 AP，以作调整。无线 AP 的布置要满足覆盖面需求，如图 10-4 所示。

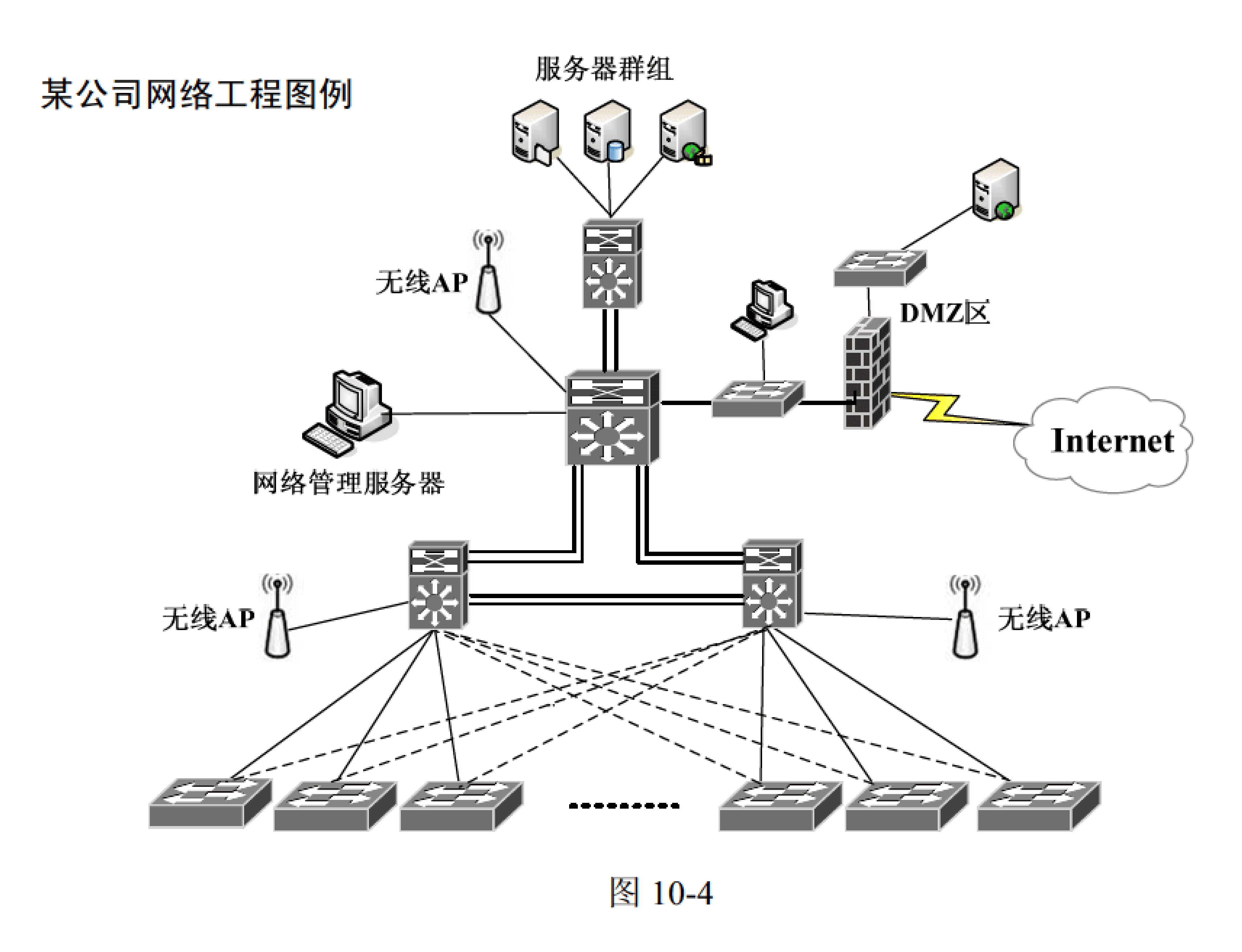


图 10-4

使用无线路由器的默认配置，无线网络会存在很多威胁，首当其冲的就是无线认证问题。默认所有用户连接无线路由器可以不用认证，这样任何一个人通过无线设备都可以很轻松的访问公司内网，这对于攻击者来说无疑是天大的好事。当然这种事是不允许发生的，所以一般都会进行无线认证连接。目前使用比较多的无线加密认证方式有 WEP 加密、WPA 加密和 WPA-PSK 安全加密算法。

WEP 无线加密算法出现比较早，由于使用的是静态密钥而非动态，导致 WEP 密码很容易被监听到或者破解。而 WPA 无线加密算法为了增强无线局域网系统的数据保护和访问控制水平，采用了动态的加密密钥，是网络业界在证明 WEP 不安全后，提出的代替 WEP 算法的一种解决方案。WPA 目前已经升级到 WPA2，是公认的比较安全的无线加密算法。但是 WPA 操作相对复杂，因此在家庭或公司的应用中经常采用 WPA 的简化版：WPA-PSK 和 WPA2-PSK。WPA-PSK 可以看成是一个认证机制，只要求一个单一的密码就可以连接到无线网络。

综上所述，在无线网络的环境中，公司有条件的话可以使用 WPA 和 WPA2 加密。如果使用了 WPA-PSK 加密方式，密码设置应该尽可能复杂，并且要注意定期更改密码。当然在选择无线加密算法的时候，还应该留意无线客户端的性能，因为较老的无线客户端，比如说无线网卡，只能支持 WEP 的加密方式，这时候无线 AP 的加密就只能选择 WEP 加密算法，可以通过尽量加大密码的长度和复杂度或者更换设备来解决。

4. 企业反病毒

病毒一直是网络安全人员的噩梦，每一次病毒冲击都能让网络管理员彻夜难眠。除了单个病毒威胁之外，病毒还有一个传播速度快的特征，一个病毒散播出去，一夜之间互联网上就会有几十万甚至上百万的用户被感染。而在企业内部，一旦有主机感染了病毒，其他主机很快也会被感染。这样依靠用户个人的杀毒软件根本无法清除干净，所以就有了企业反病毒系统。

企业反病毒系统主要由两部分组成：企业版杀毒软件和管理控制台。需要在每一台客户机、服务器上安装企业版杀毒软件，同时要找一台管理机安装管理控制台工具。用户可以使用本机的企

业版杀毒软件进行病毒扫描、查杀，同时也可以由管理员借助管理控制台进行全网病毒监控和全网病毒查杀。借助管理控制台还可以定制网络病毒扫描、查杀计划任务。

常见的企业反病毒系统有诺顿、ESET NOD32、卡巴斯基、360、趋势科技等。各个厂商的产品都有自己的优势，且配置方法略有不同。改造后的网络拓扑图如图 10-5 所示。

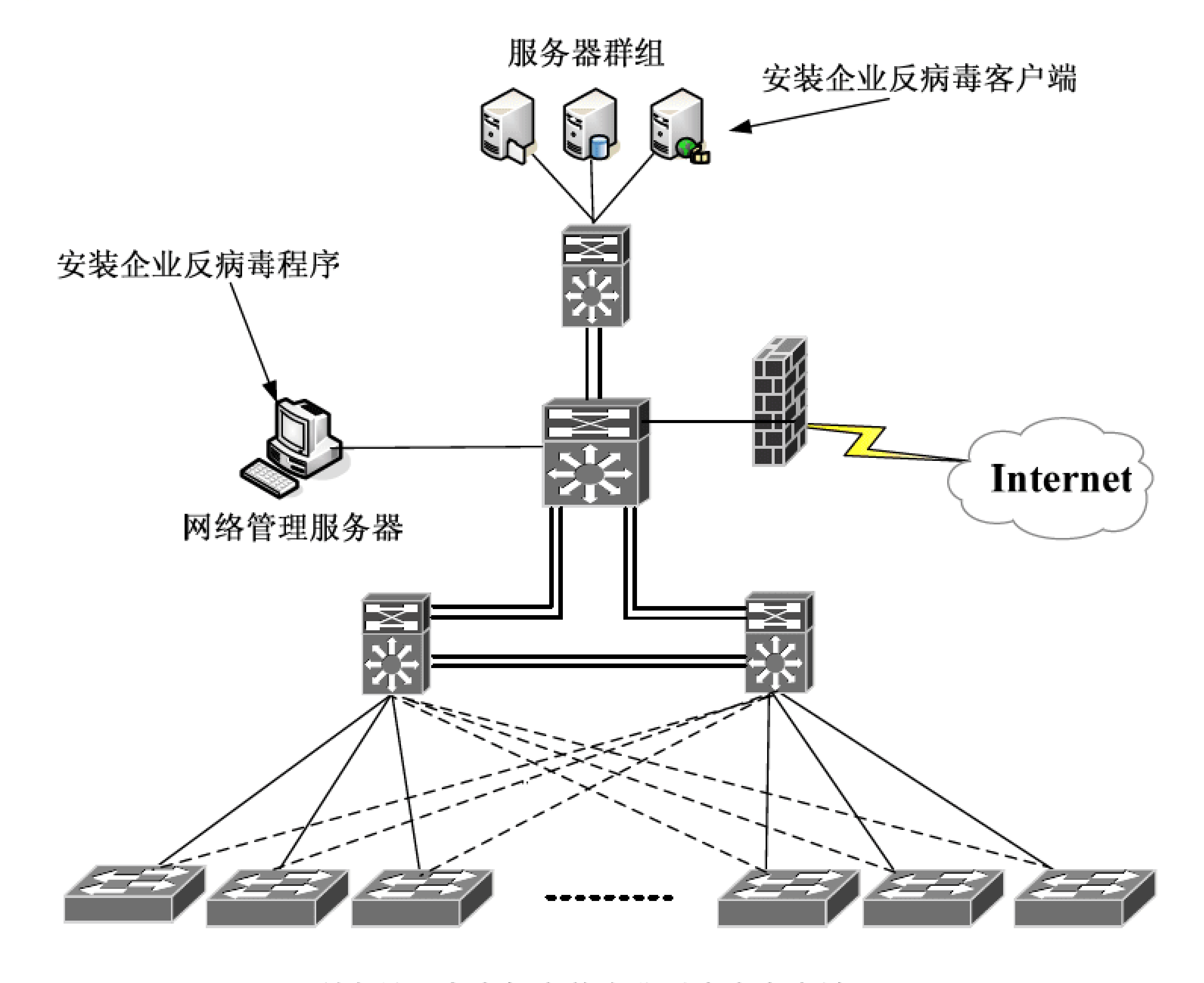


图 10-5

10.3.2 网络出口安全

企业内部网络的安全，绝大部分需要依靠网络出口的安全设置。一般网络出口在做安全配置时会采用防火墙、防毒墙、基于网络的入侵检测三项技术。防毒墙可以是一款硬件设备，因为本案例已经采用了企业防病毒系统，所以在网络出口没有配置防毒墙。下面详细介绍企业防火墙和入侵检测系统的实施方法。

1. 企业防火墙

企业网络现状是只有内外两个出口的双向防火墙，防止了外部网络的攻击，但是企业大部分的对外发布服务都放在了 IDC 机房托管服务器上，不利于重要数据的安全防护，所以在改造时，将企业重要信息服务放到内网对外发布。

由于企业内网用户群比较大，信息相对混杂，如果直接和企业内部服务器放在一起，会有安全隐患。所以这里借助防火墙的 DMZ（隔离区），将对外发布服务器安全隔离，这样内外网都可以访问该服务器，同时也不会造成安全威胁。

上述部署需要出口防火墙支持 DMZ 接口配置，其实大部分的硬件防火墙都支持该功能，如果出口使用计算机安装的软件防火墙，多增加一块网卡即可。

环境配置好之后，最主要的还是访问规则的配置，在配置防火墙时默认所有流量都不允许通

过，只需将必须的流量配置为转发即可。不同的企业访问规则要求也不相同，一般会有以下几点。

（1）允许内部员工访问 DMZ 区服务器和外部互联网。

（2）发布 DMZ 区服务器，允许外部网络对其进行访问。

（3）限制员工的网络访问时间及访问权限，禁止访问游戏、娱乐型网站，如开心网、QQ 农场等。

（4）限制员工的视频流量、BT 或迅雷下载流量，减少带宽浪费。

（5）允许网络管理员远程监控防火墙，限制其他员工访问。

目前企业使用比较多的防火墙有 ISA Server 2006、Cisco ASA 5500 系列、天融信、华为赛门铁克等。除了 ISA Server 2006 以外，大部分都是硬件防火墙。虽然产品不同，但是配置规则大同小异。改造后的网络拓扑图如图 10-6 所示。

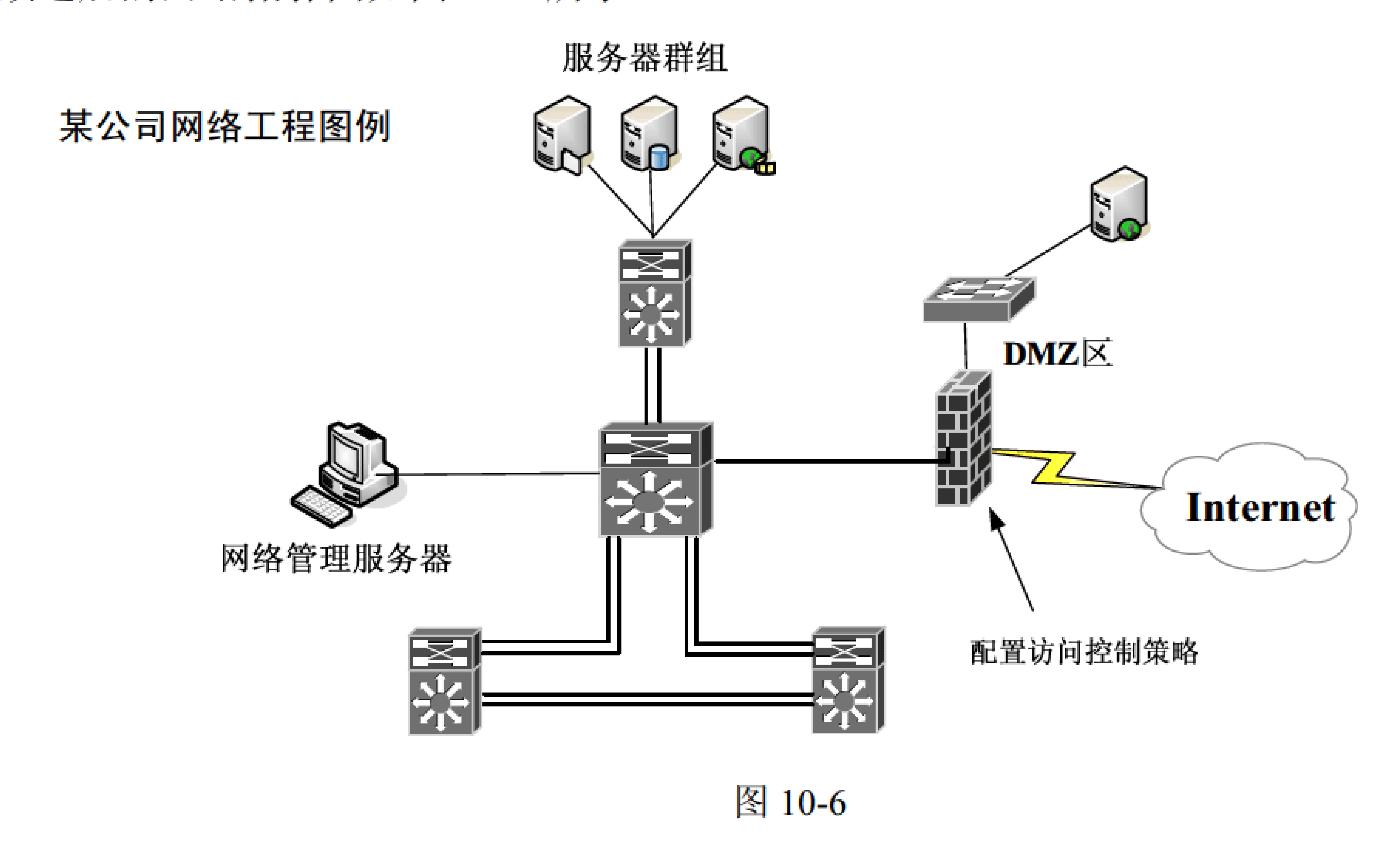


图 10-6



由于在这一步才加入 DMZ 区，所以 DMZ 区的服务器需要在此单独加入基于主机的入侵检测系统和企业反病毒系统客户端。

2. 基于网络的入侵检测系统

对于企业网络来说，除了病毒威胁，另一个就是网络攻击了。企业网络无时无刻不在承受网络攻击的威胁，特别是知名大公司。

对于网络攻击，防火墙可以起到很大的防护作用，但是对于安全级别要求很高的企业来说，这远远不够。很多网络攻击利用加壳隐藏的方式，可以逃避防火墙的扫描。而且很多防火墙只能做到分析传输层以下的信息，如果利用的是应用层攻击，防火墙不一定能够有效，所以增加补充技术是必须的，这里主要的补充技术是基于网络的入侵检测系统。

通常需要对防火墙过滤的数据流进行二次扫描过滤，可以在防火墙后端直接加入一台入侵检测系统。入侵检测系统有软件、硬件两类产品，本案例采用的是软件，通过交换机连接一台入侵检测系统来实现安全过滤。改造后的网络拓扑图如图 10-7 所示。

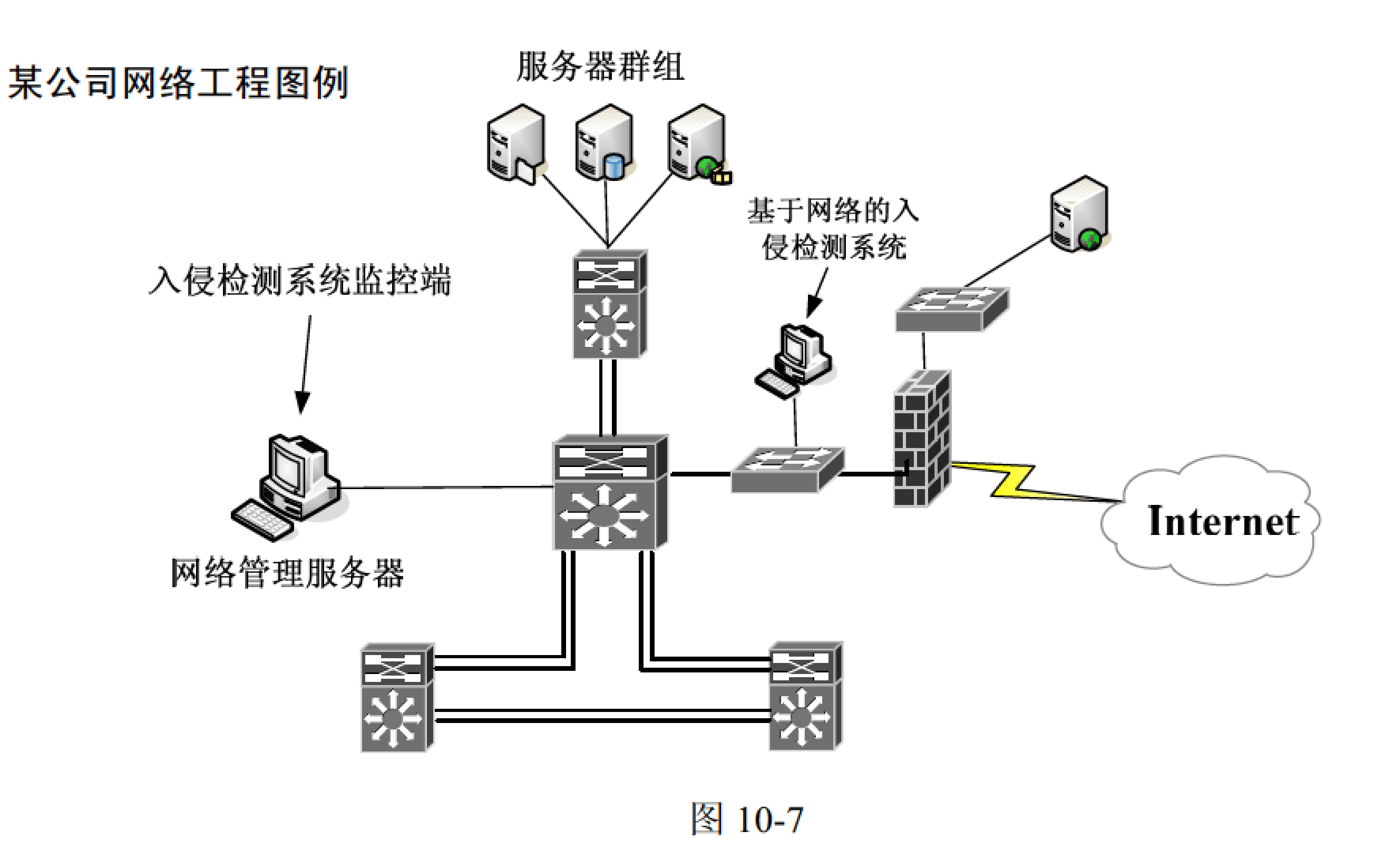


图 10-7

10.3.3 远程用户的安全接入

对于子公司、移动及家庭办公员工来说，需要经常和企业内部网络进行通信，访问内部网络服务器或者和内部员工交流信息，有时可能还会进行视频会议。这些流量直接通过简单的互联网连接到企业网络，根本无法保证其安全，所以需要寻求一种安全加密的连接手段。

VPN（虚拟专用网）技术，可以在不改变现有网络连接结构的情况下，在总公司防火墙到子公司或在外移动办公员工之间建立一条加密的虚拟隧道连接。通过这种连接方法可以让这些网络用户和总公司连接时像是局域网互联一样。外部网络攻击者很难窃取使用这种方法传输的通信信息。

在实施时，移动或家庭办公员工不需要长期保持连接，可以使用远程访问 VPN 连接。而子公司和总公司通信频繁，需要使用 IPSec VPN 保持长期的连接。

配置时，可以在网络出口外连接使用专业的 VPN 设备，也可以使用出口防火墙或路由器自带的 VPN 功能。改造后的网络拓扑图如图 10-8 所示。

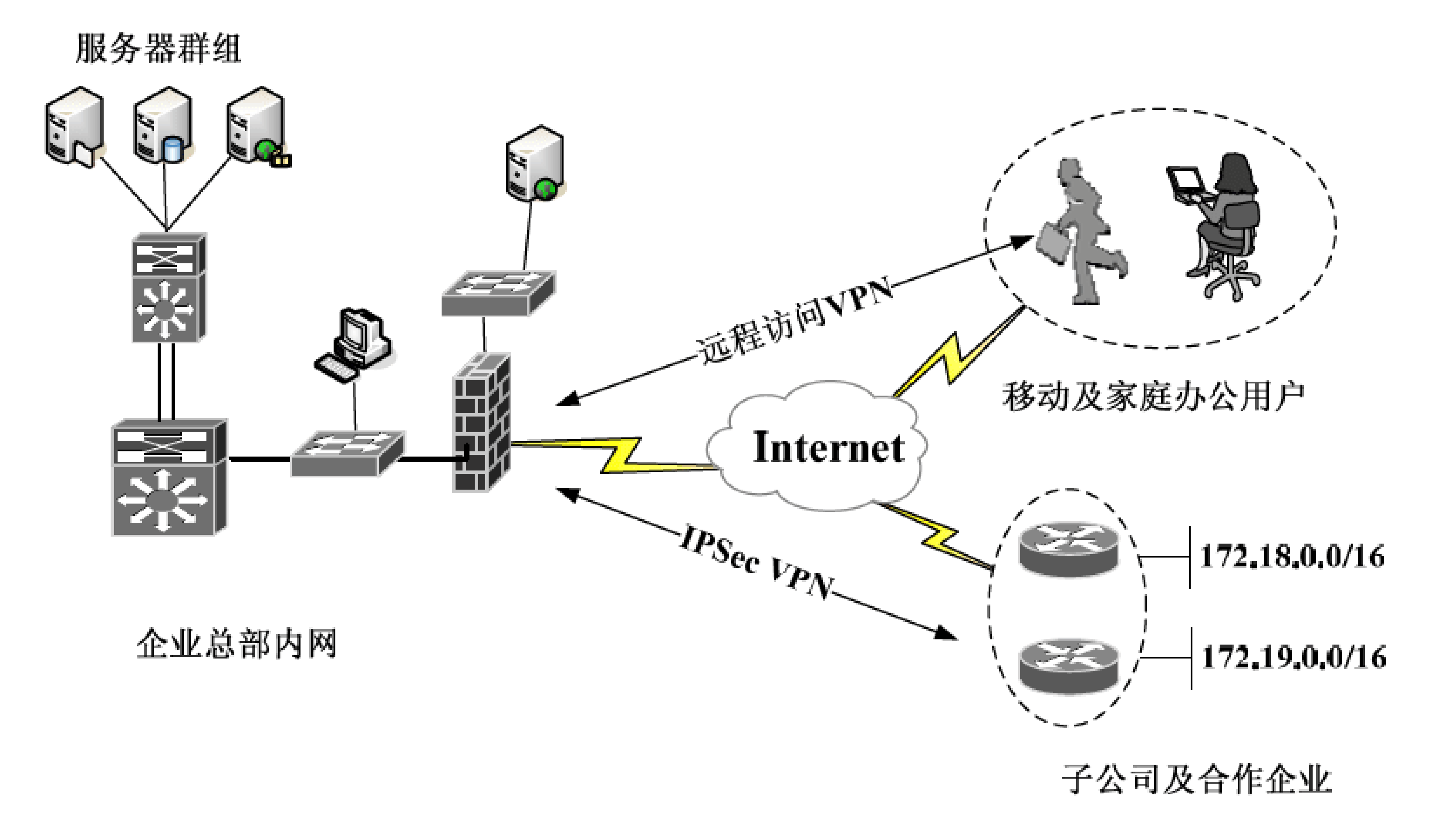


图 10-8

10.4　专家答疑

（1）是不是按照以上方案配置必要的安全设备就可以保证网络安全了？

答：随着信息技术飞速的发展，任何技术都不可能是完美的，所以也不可能存在绝对安全的网络，除非将企业网络和互联网彻底物理隔离。

服务器、网络设备会不断的有新漏洞产生，每一个漏洞都有可能被网络攻击者利用。网络环境在使用中也会不断的变化，如果不加注意很容易在使用中增加安全隐患。作为网络管理员，不可能绝对的保证网络安全，但是却可以通过及时的网络更新、漏洞扫描、流量分析等操作降低安全威胁。同时网络管理员也需要不断的学习新技术，了解各种攻击手段，使网络安全防护更有针对性。

（2）是不是所有网络都需要布置本案例的安全技术呢？

答：本案例的安全技术只是普通网络的通用安全解决方案，并不是所有网络的安全部署都相同，需要根据当前的网络环境、业务需要做调整。但是，大体上用到的还是这些技术，只是技术应用或部署的方法有所改变。

比如证券、银行等机构有很多小的办事点，特别是银行有很多 ATM 取款机，这些小网点互联时使用的可能还是 VPN 技术，但却不一定会使用 IPSec VPN 了。一般使用 MPLS VPN，这种 VPN 技术可以按照流量收费，不需要 ATM 机做其他网络连接。

又比如，大型企业网的防火墙只依靠一个带 DMZ 区的三向防火墙可能不能满足安全需求，需要配置更安全的防火墙方案，如高可用性的双核心防火墙或高安全性的前后端防火墙。

再比如，有些网络没有重要的服务器，网络安全级别要求比较低。这样的网络可能就不需要基于主机的入侵检测系统，甚至连基于网络的入侵检测系统也不需要。

所以网络安全方案要完全依照自身网络的需求进行设计。

第 11 章　Windows Server 2008 系统安全

Windows Server 2008 是微软推出的新一代服务器操作系统，和 Windows Server 2003 操作系统相比，不仅功能上有了很大的提升，而且在系统安全性上也得到了很大的提高。Windows Server 2008 的安全性主要涉及到系统安全、防火墙安全、端口安全和策略安全等，当然系统管理员需要根据实际情况来启用不同的安全策略。

11.1　Windows 系统漏洞安全

系统漏洞是指应用程序或者操作系统在设计上的缺陷，从理论上讲系统漏洞是不可避免的。但这些漏洞缺陷常常会被非法用户利用，有些甚至将木马、病毒等有害程序安装在服务器中，窃取服务器数据，因此及时地进行漏洞扫描是保证服务器安全性的有效措施之一。

11.1.1　系统漏洞扫描

对于 Windows 系统而言，在操作系统安装完成或者是系统升级后都会产生漏洞，这时候就需要对系统进行漏洞扫描，然后对高危害性漏洞及时打补丁，以增加系统的安全性和可靠性。MBSA（Microsoft Baseline Security Analyzer）又叫微软基准安全分析器，可以扫描系统漏洞。

1. 安装 MBSA 软件

安装 MBSA 软件的具体操作步骤如下。

01 双击 MBSA 安装文件，弹出【MBSA Setup】（MBSA 安装）对话框，显示 MBSA 安装信息，单击【Next】（下一步）按钮，如图 11-1 所示。

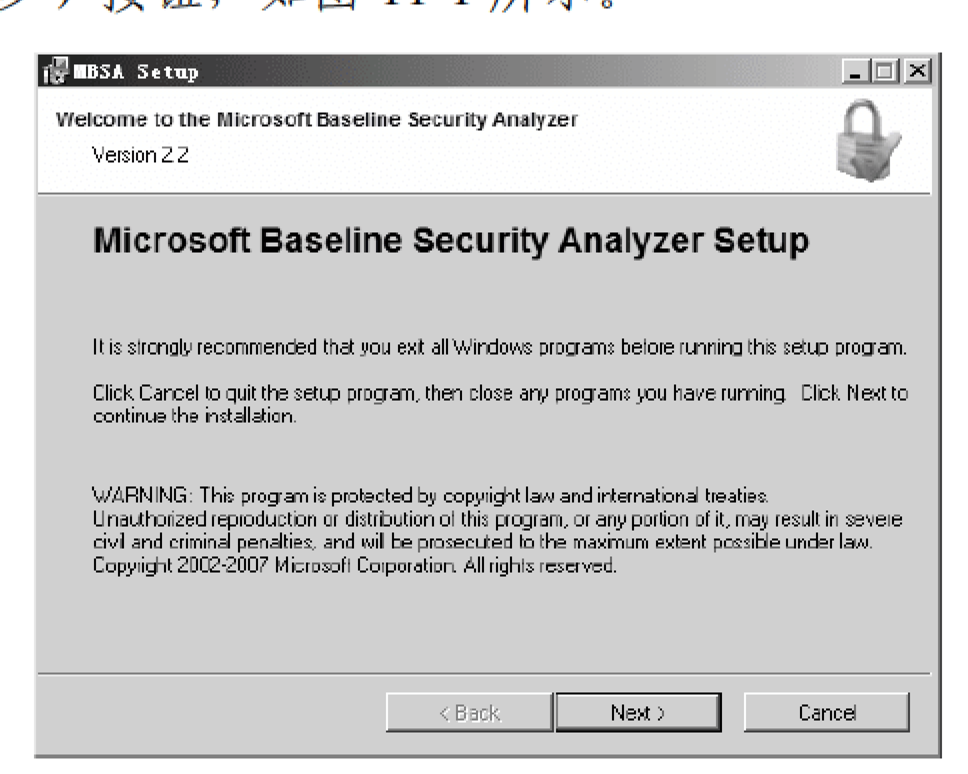


图 11-1

02 弹出【License Agreement】（许可协议）对话框，显示 MBSA 的安装协议，选择【I accept

the license agreement】（我接受许可协议）单选框，单击【Next】（下一步）按钮，如图 11-2 所示。



图 11-2

03 弹出【Destination Folder】（安装目录）对话框，单击【Browse】（浏览）按钮，自定义 MBSA 的安装路径，这里选择默认安装路径为“C:\ProgramFiles\Microsoft Baseline Security Analyzer\”，单击【Next】（下一步）按钮，如图 11-3 所示。



图 11-3

04 弹出【Start Installation】（开始安装）提示框，提示上面填写的安装信息是否正确，单击【Install】（安装）按钮，如图 11-4 所示。

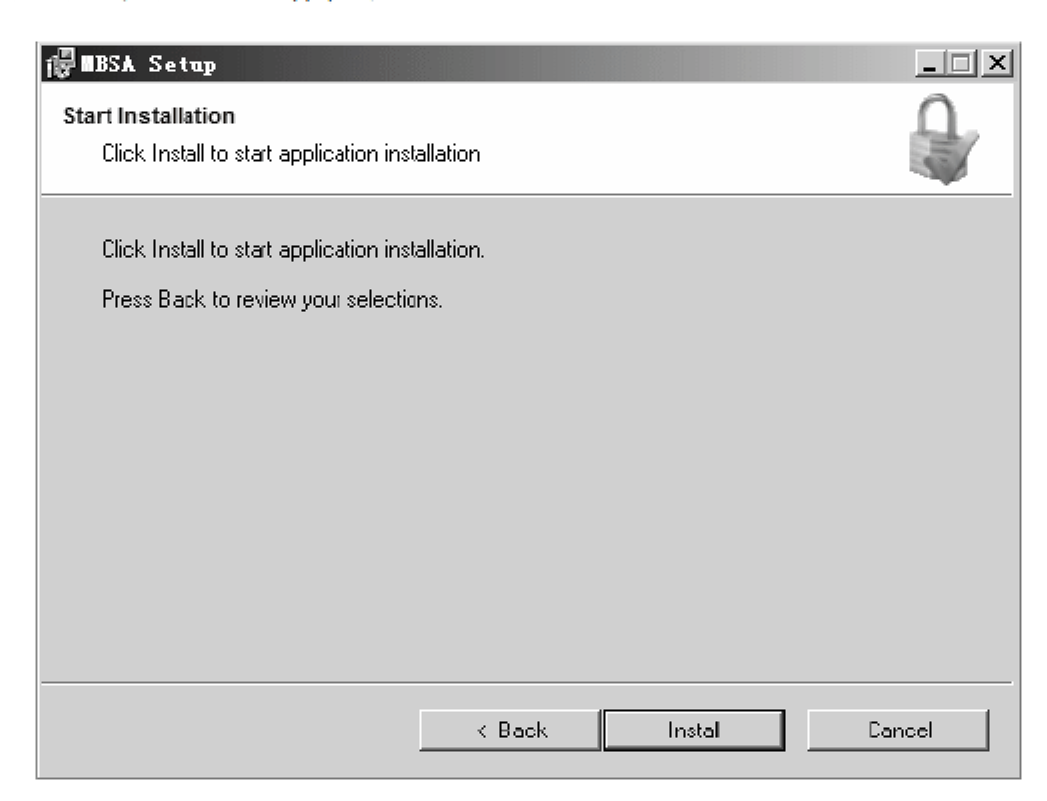


图 11-4

05 弹出【MBSA Setup】（MBSA 安装）提示框，单击【OK】（确定）按钮，完成 MBSA 的安装，如图 11-5 所示。

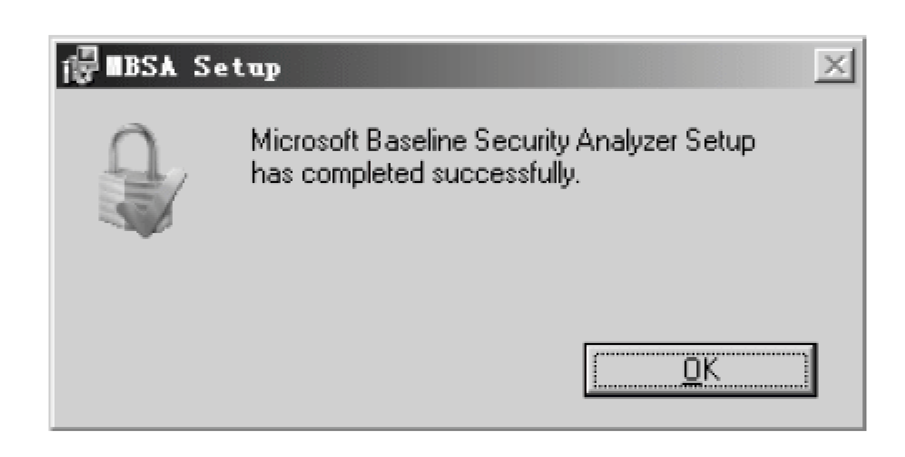


图 11-5

2. 利用 MBSA 进行漏洞扫描

利用 MBSA 进行漏洞扫描的具体操作步骤如下。

01 选择【开始】➢【所有程序】➢【Microsoft Baseline Security Analyzer】菜单命令，打开 MBSA 软件，单击左侧【Scan a computer】(扫描一个计算机)菜单，表示要扫描一个计算机，如图 11-6 所示。

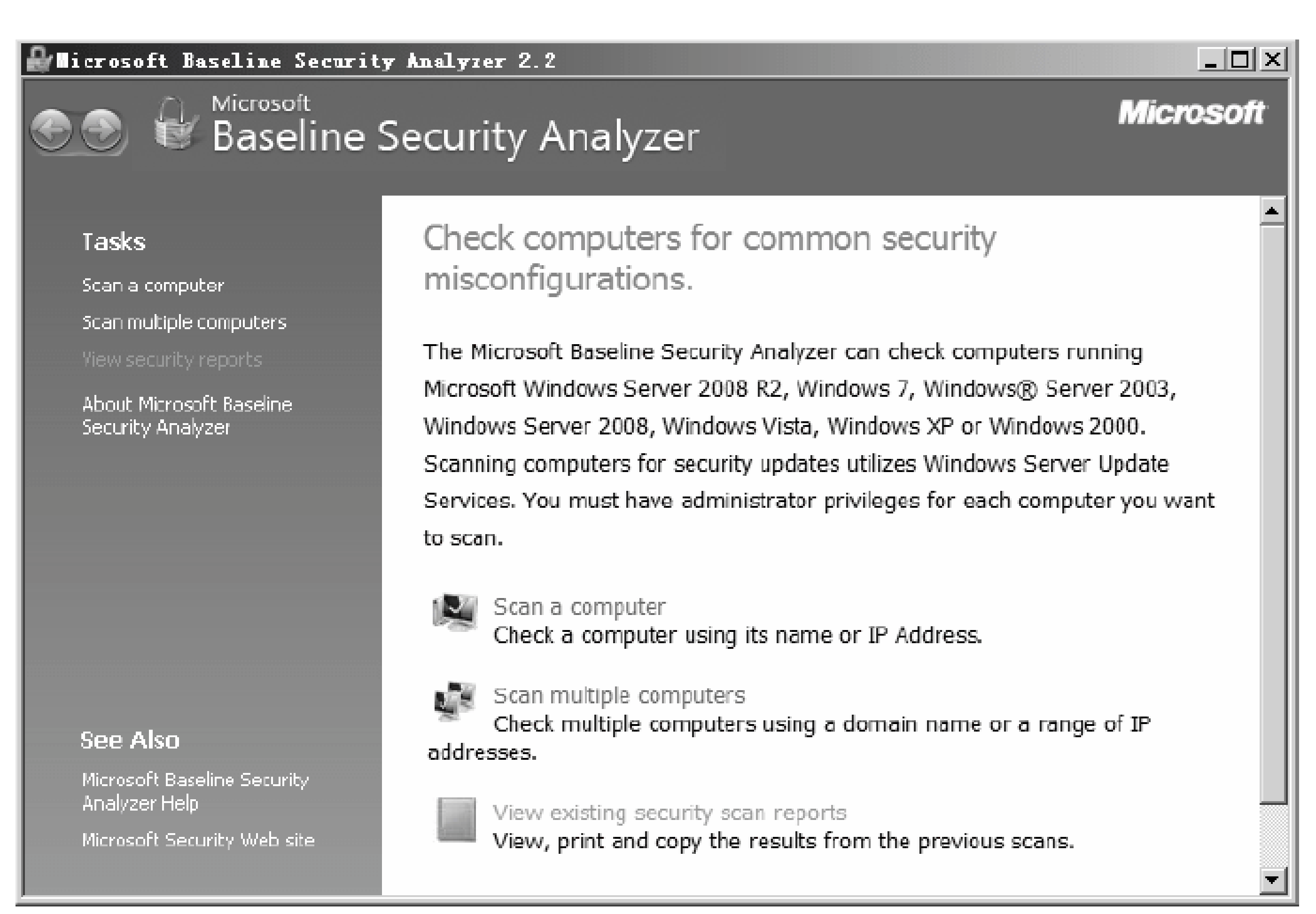


图 11-6

02 弹出【Which computer do you want to scan】（将要扫描哪台计算机）窗口，在其中输入扫描计算机的信息。在【IP address】（IP 地址）文本框输入要扫描的计算机的信息，这里输入“192.168.1.104”，单击【Start Scan】（开始扫描）按钮，如图 11-7 所示。

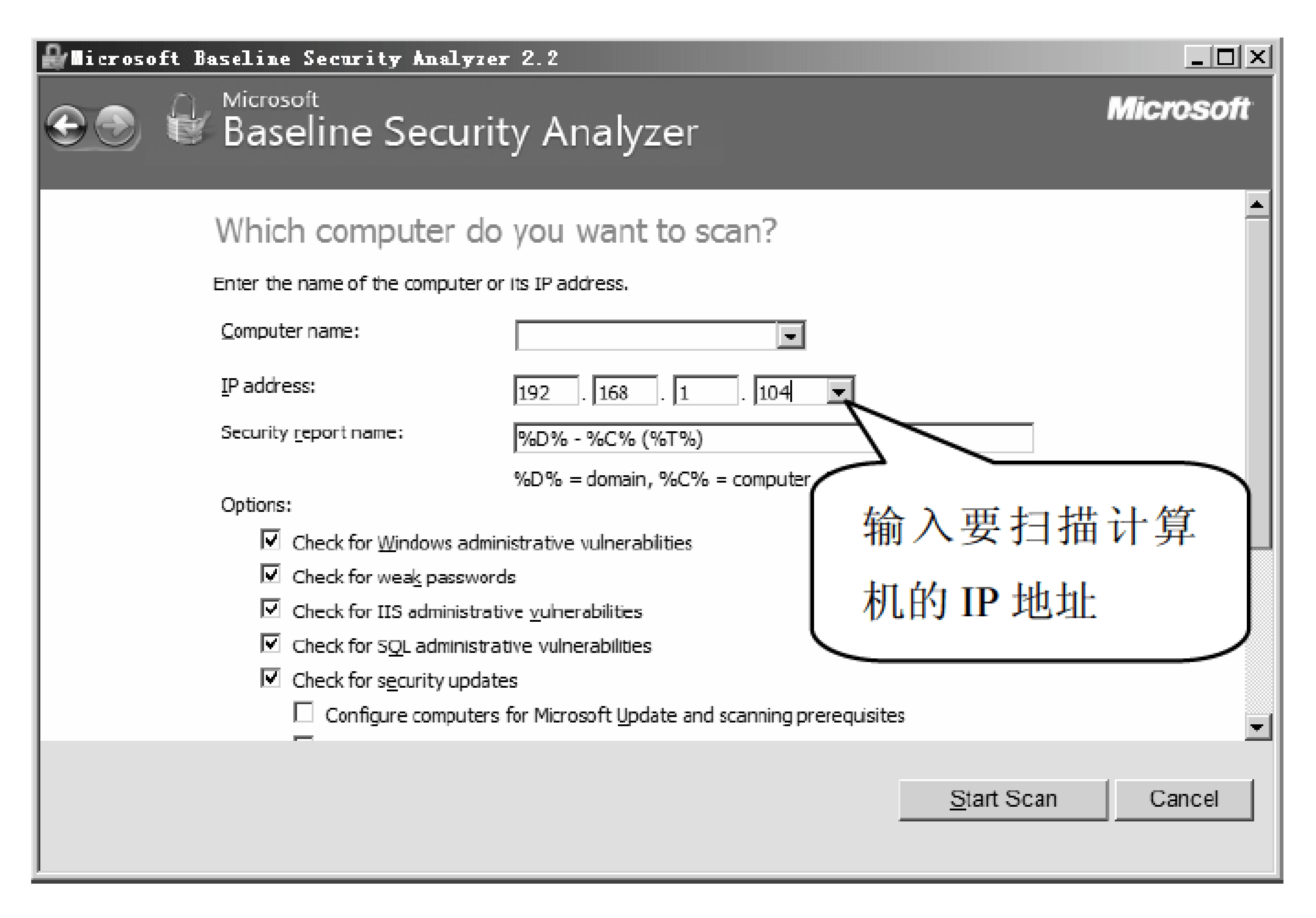


图 11-7

03 弹出【Scanning…】（扫描）窗口，提示 MBSA 正在从微软官网下载安全升级信息，如图 11-8 所示。

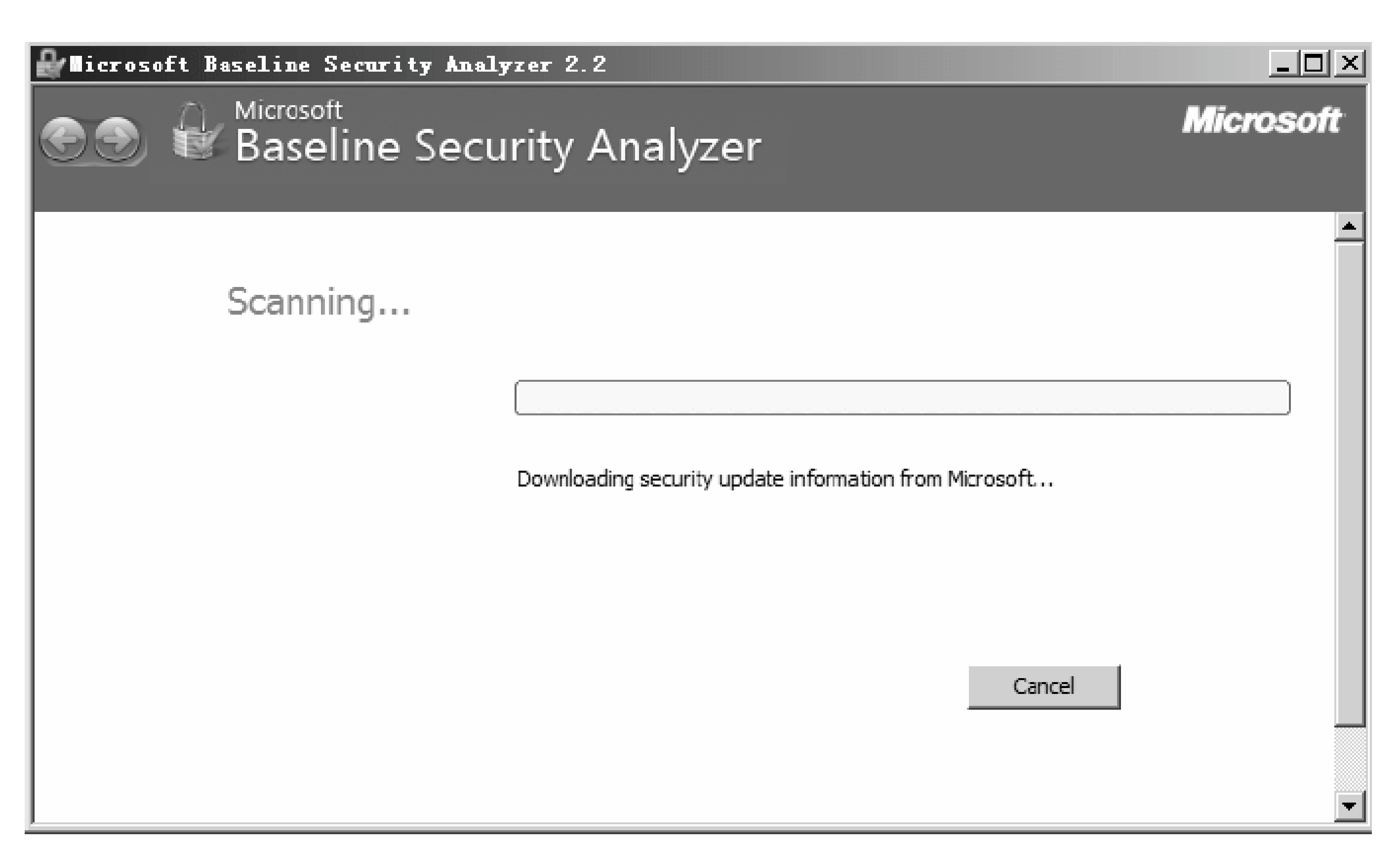


图 11-8

04 升级完毕后，打开新页面，提示 MBSA 软件正在对名称为【WIN-013D26R8BJX】的计算机进行扫描，如图 11-9 所示。

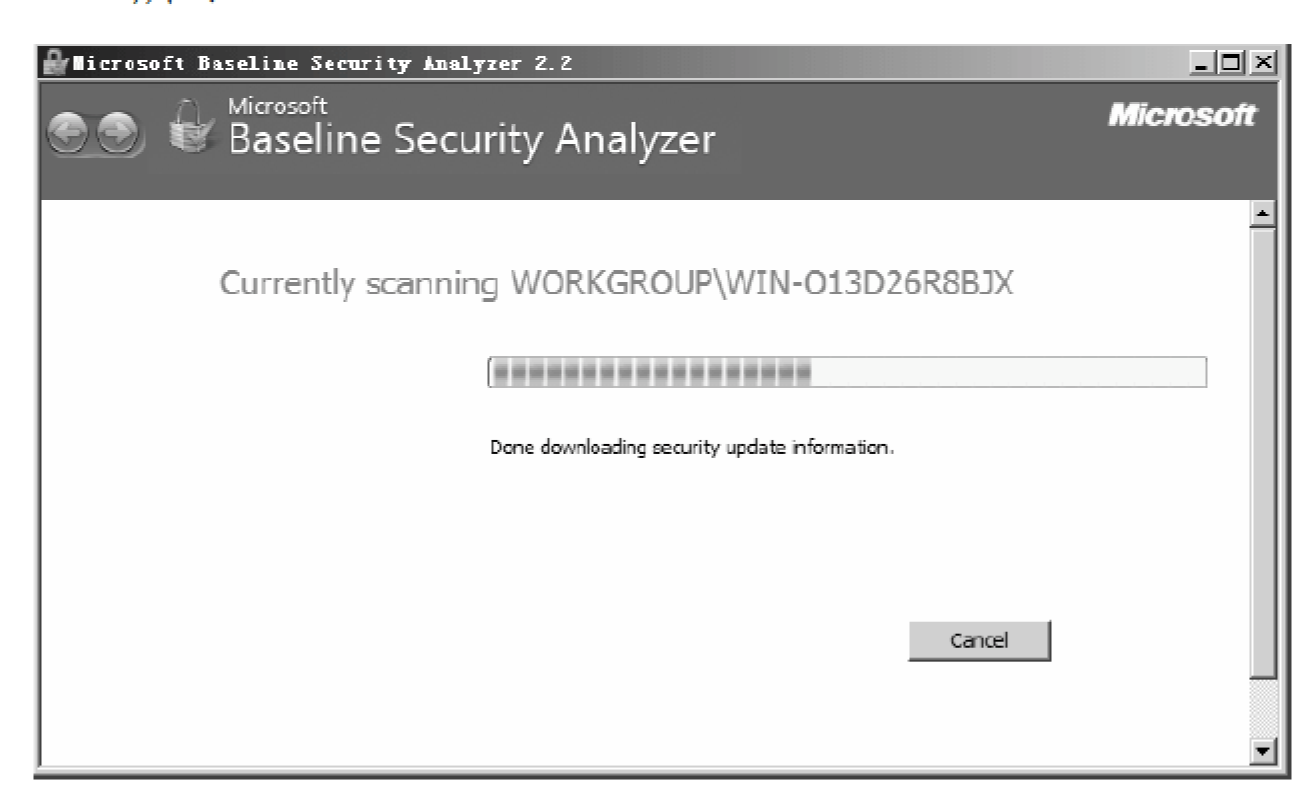


图 11-9

05 扫描完成，显示扫描结果信息。滚动页面，显示出扫描到的目标主机的问题。在【Issue】（问题）列显示的是扫描的是 Windows 安全信息还是 SQL Server 安全信息；在【Result】（结果）列显示扫描的问题。单击【Windows Security Updates】（Windows 安装更新）行后的【Result details】（扫描结果信息报告）超级链接，如图 11-10 所示。

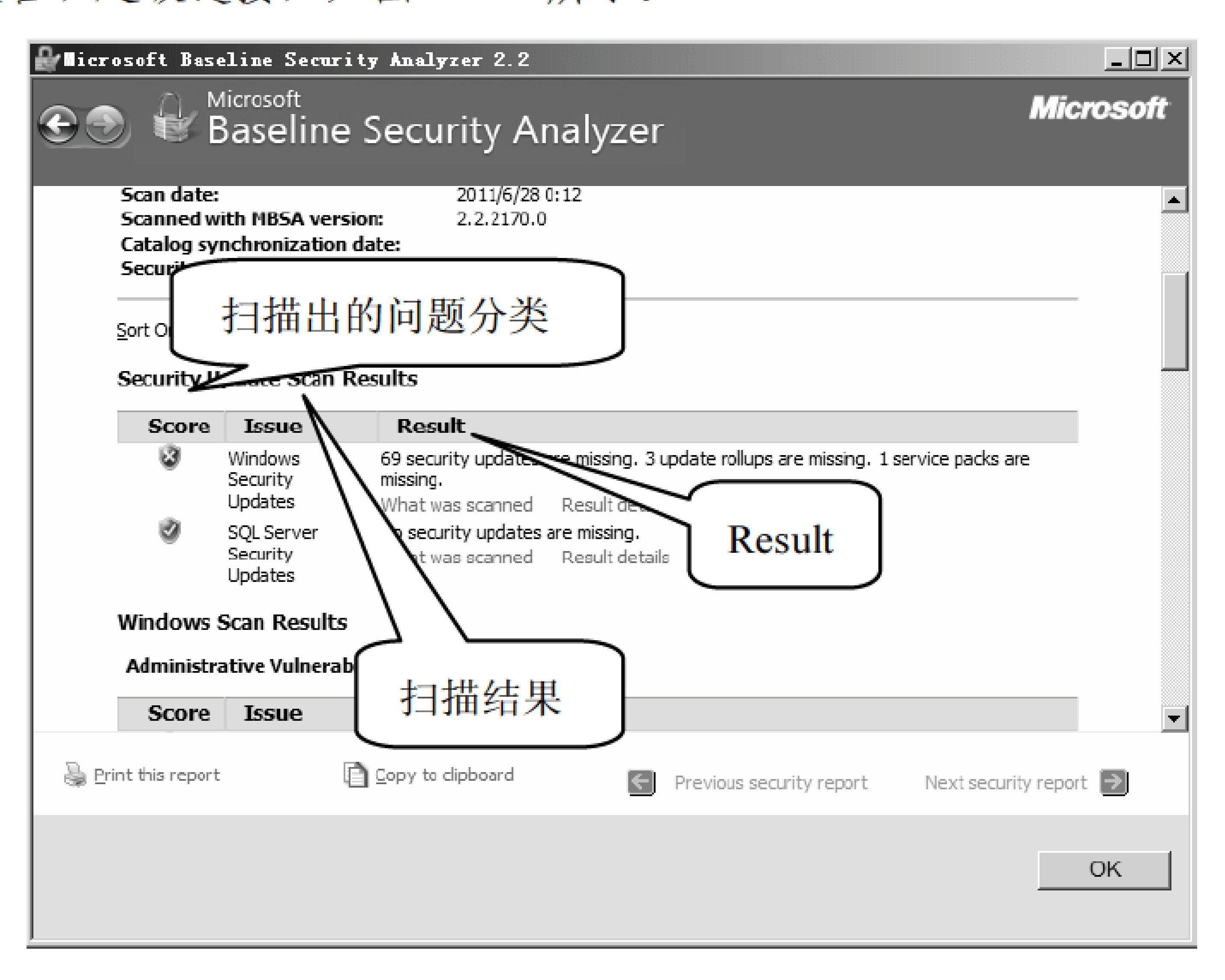


图 11-10

06 弹出新窗口，显示 Windows 系统的漏洞信息。单击要安装的补丁超链接，这里单击第一个补丁超级链接，如图 11-11 所示。



图 11-11

07 弹出【微软的安全更新】网页，可以根据系统的版本等信息来决定下载的补丁，然后进行补丁安装，如图 11-12 所示。

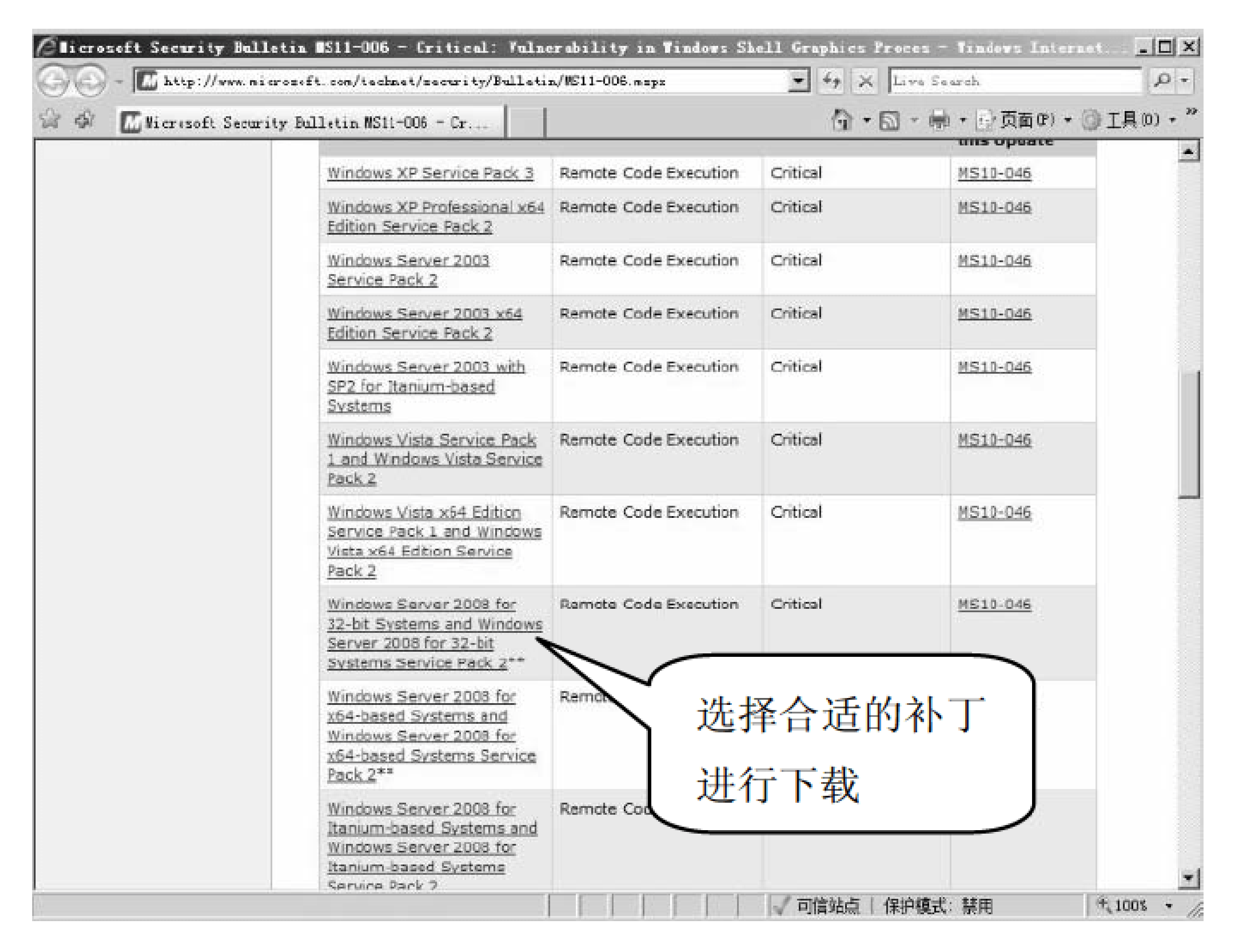


图 11-12

08 单击【Windows Security Updates】（Windows 安装更新）行后的【How to correct this】（如何正确的去做）超级链接，如图 11-13 所示。

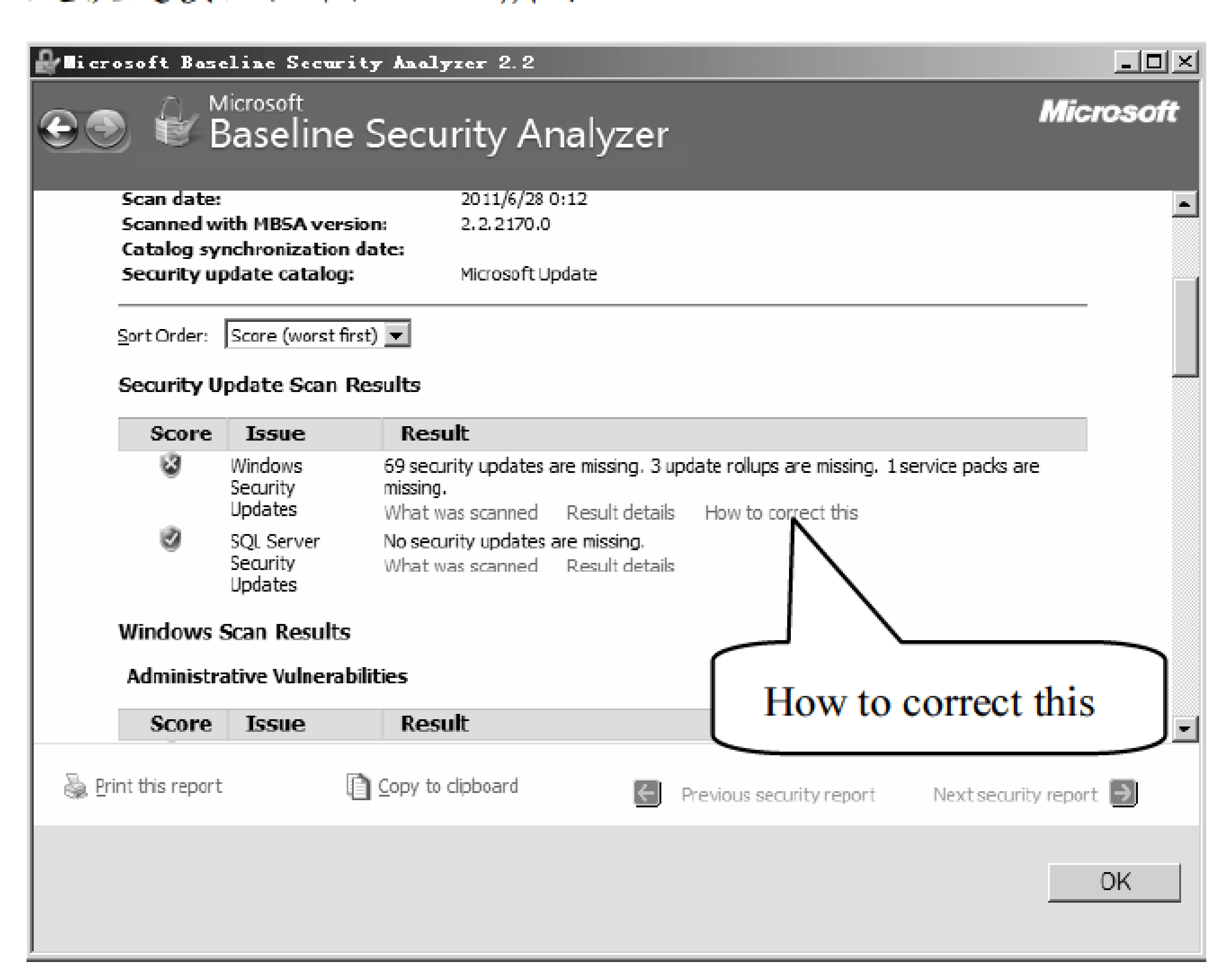


图 11-13

09 弹出网页扫描报告，告诉用户如何解决该安全问题，如图 11-14 所示。

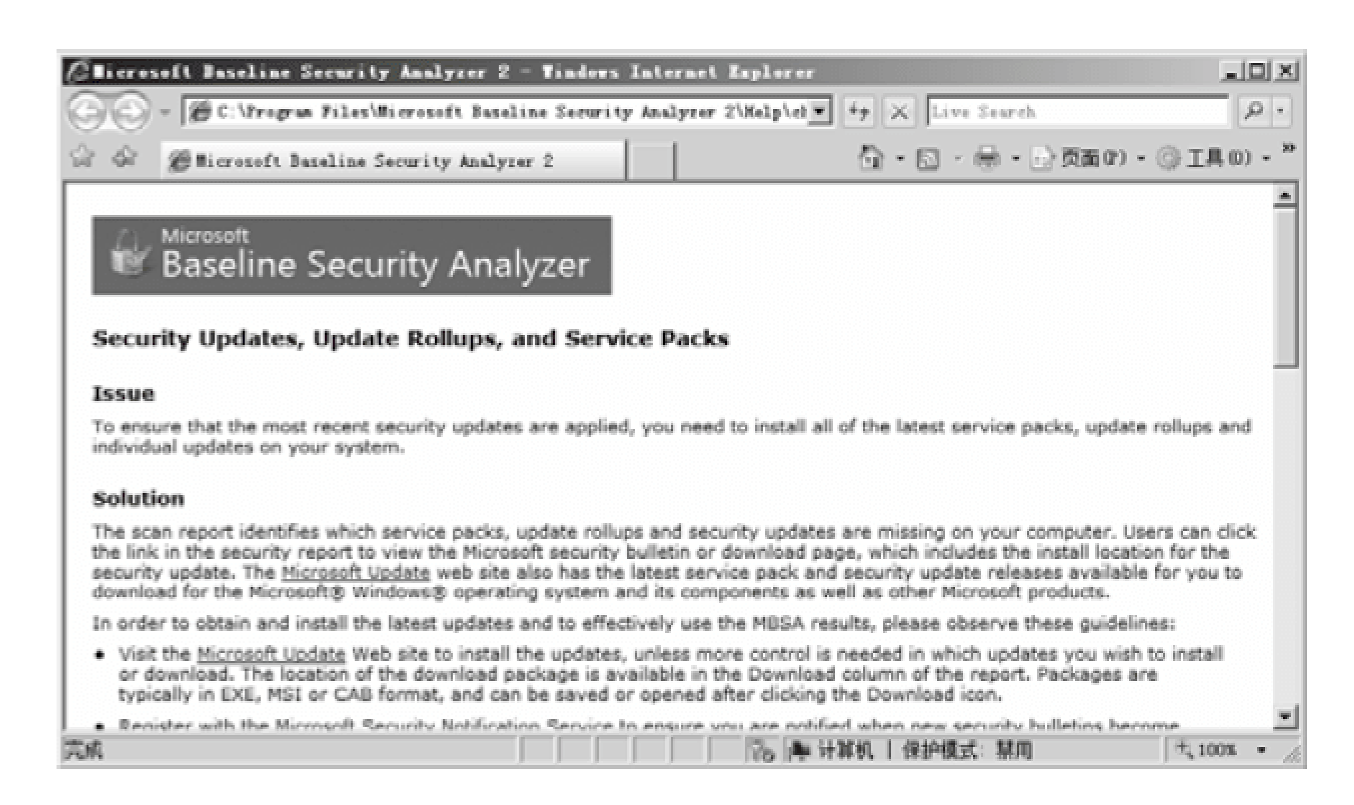


图 11-14

10 在扫描结果页面中单击【OK】（确定）按钮，可以关闭扫描结果窗口。

11.1.2 漏洞修补策略

系统管理员发现漏洞后，应该及时进行漏洞修补，但是所有的漏洞都需要安装修补吗？不是的。用户应该根据不同的系统，不用的应用和补丁的具体功能来决定是否需要打该补丁，否则如果给系统安装了不适合的补丁，不仅解决不了系统安全问题，反而有可能造成不可弥补的损失，在安装补丁的时候应该注意以下信息。

1. 及时备份数据

在系统安装补丁或者系统更新之前最好及时进行数据备份，以免因为漏洞补丁的问题，造成系统错误或者数据丢失。一般情况下应该在安装补丁之前及时对补丁安装相关分区的数据和系统 DLL 链接库的文件进行备份。

2. 检查补丁信息

在安装补丁之前，首先应该查看该补丁说明，以掌握补丁用途；然后查询补丁安装需求，因为补丁一般是针对特定的产品的；最后应该查询补丁危害等级，验证服务器是否必须安装该补丁。

3. 选择补丁下载方式，确保补丁真实可靠

现在有很多的漏洞扫描工具，可以对系统的漏洞进行扫描并自动进行补丁更新操作。但是对于服务器来说，为了保证服务器的稳定性，在安装补丁之前，应该考虑补丁是直接从互联网下载，还是下载到本地后在安装到服务器上。一般来说，从微软官网下载的补丁都是安全可靠的。

11.1.3 系统更新

Windows Server 2008 系统为用户提供了系统更新的功能，该功能的主要作用就是自动进行系统和应用程序的升级更新，进而提高系统安全性。

设置系统更新的具体操作步骤如下。

01 选择【开始】➢【控制面板】菜单命令，打开【控制面板】窗口，单击【Windows Update】图标，如图 11-15 所示。



图 11-15

02 打开【Windows Update】窗口，单击【立即启用】按钮，开始系统更新，如图 11-16 所示。



图 11-16

03 系统更新程序正在检查系统更新，如图 11-17 所示。

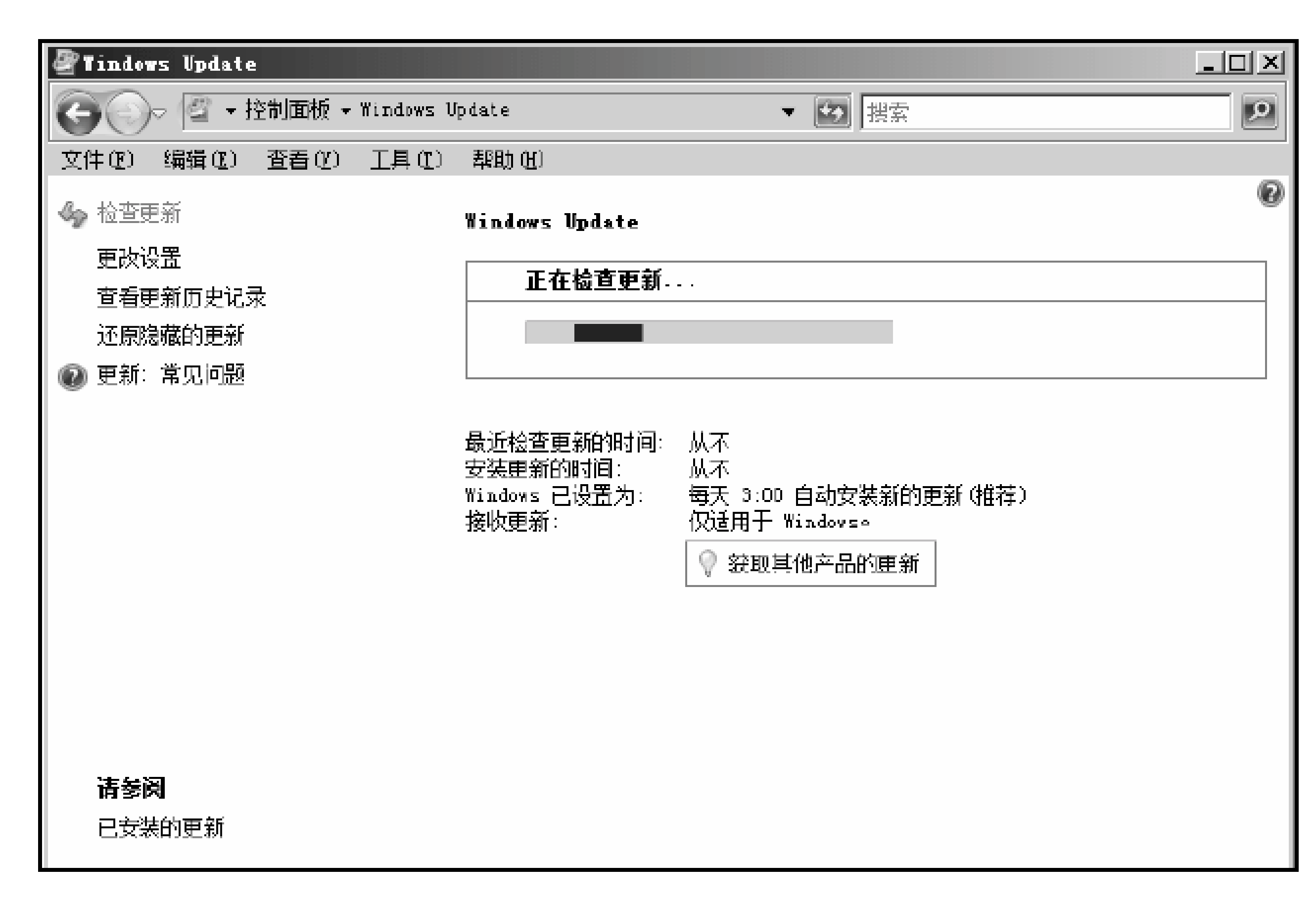


图 11-17

04 系统更新检测完成后，单击【现在安装】按钮，开始安装系统更新，如图 11-18 所示。

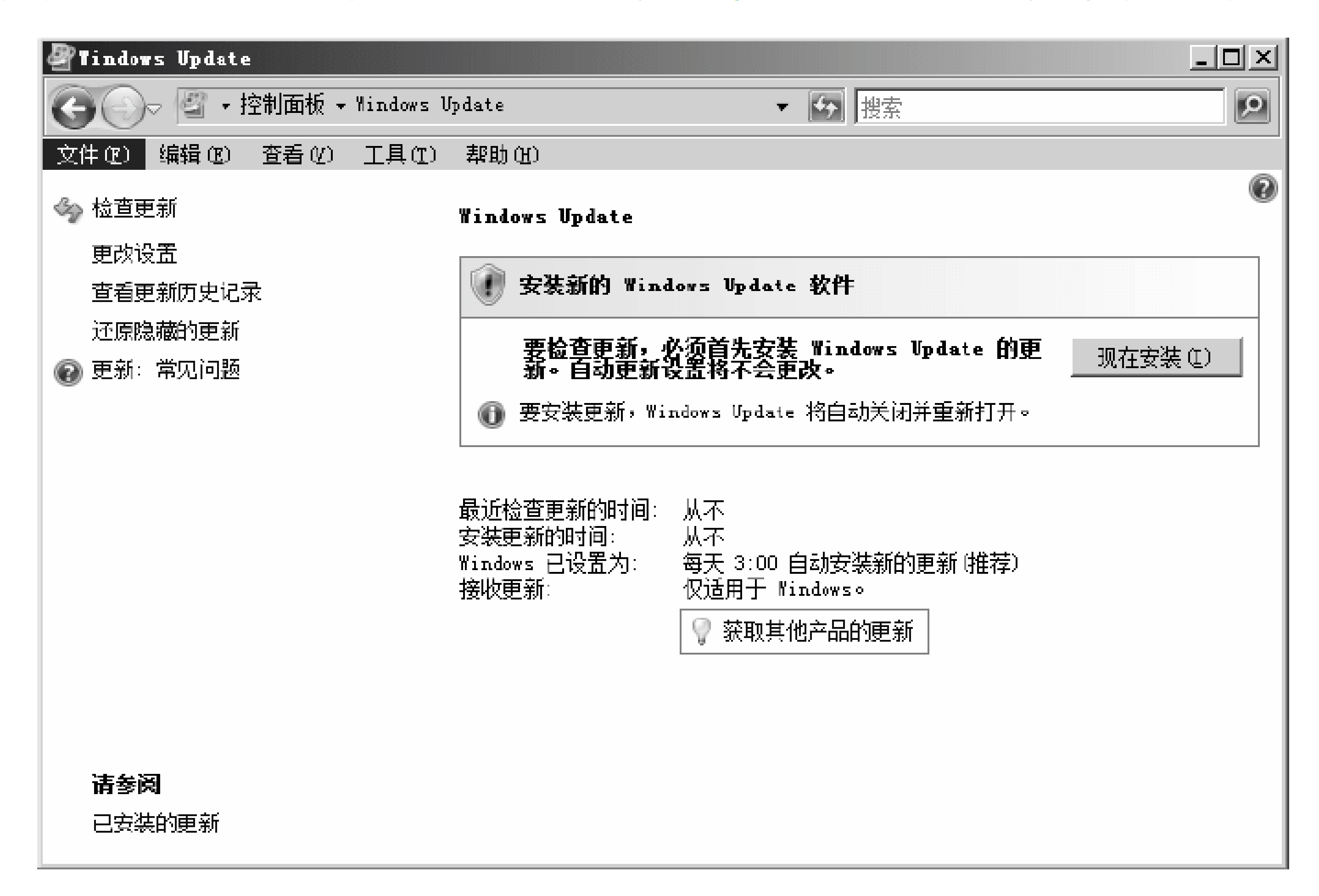


图 11-18

05 系统正在下载并安装更新，显示下载和安装进度条。安装完成后，单击左侧【更改设置】选项，如图 11-19 所示。



图 11-19

06 弹出【更改设置】对话框，在【安装新的更新】文本框中输入自动安装更新的时间，本实例中输入每天 3:00，表明在以后每天 3:00 系统自动扫描漏洞然后进行更新，单击【确定】按钮，如图 11-20 所示。

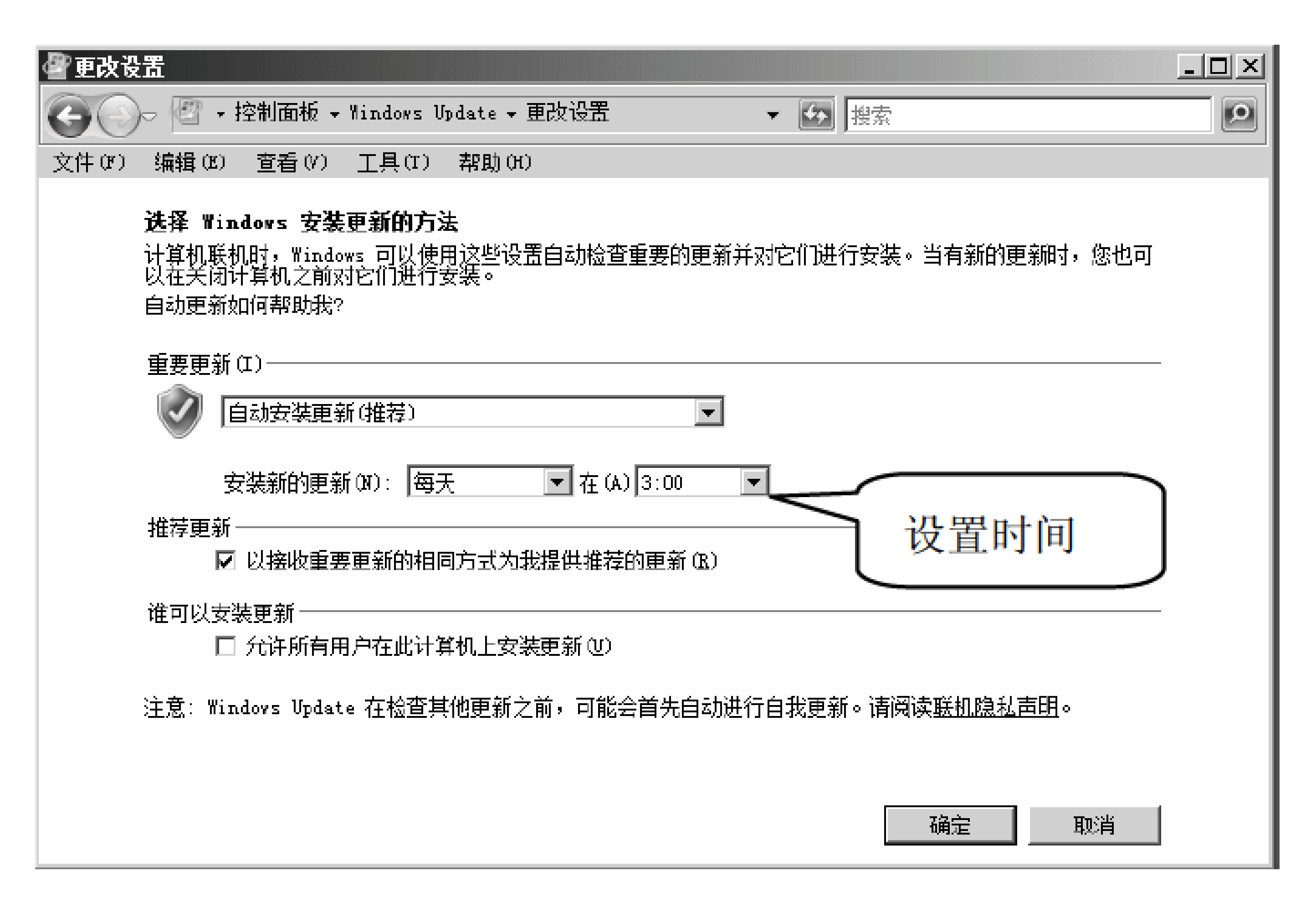


图 11-20

11.2 Windows 端口安全

端口又叫通信端口，是计算机与计算机之间通信的出口。在互联网中 IP 地址可以帮助计算机连接到另外一台计算机上，但是必须借助于端口才能访问目的计算机的特定服务。计算机上的服务使用的端口是不能重复的，比如默认情况下 Web 服务器使用的端口是 80，FTP 服务器使用的端口是 21 等，很多服务器遭受到攻击，就是因为黑客利用计算机开启的端口进行了攻击。因此，系统管理人员必须掌握常见端口的使用方法，以及如何开启和关闭某个端口。

11.2.1 查看使用端口

一般来说，服务器上只开启必须运行的服务需要的端口，其他的端口一律关闭。在关闭端口之前首先应该查询系统开启了哪些端口。

1. 查看当前有哪些计算机正在和本机连接，包括使用的 IP 地址、端口等信息

信息查看的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“cmd”命令，单击【确定】按钮，如图 11-21 所示。

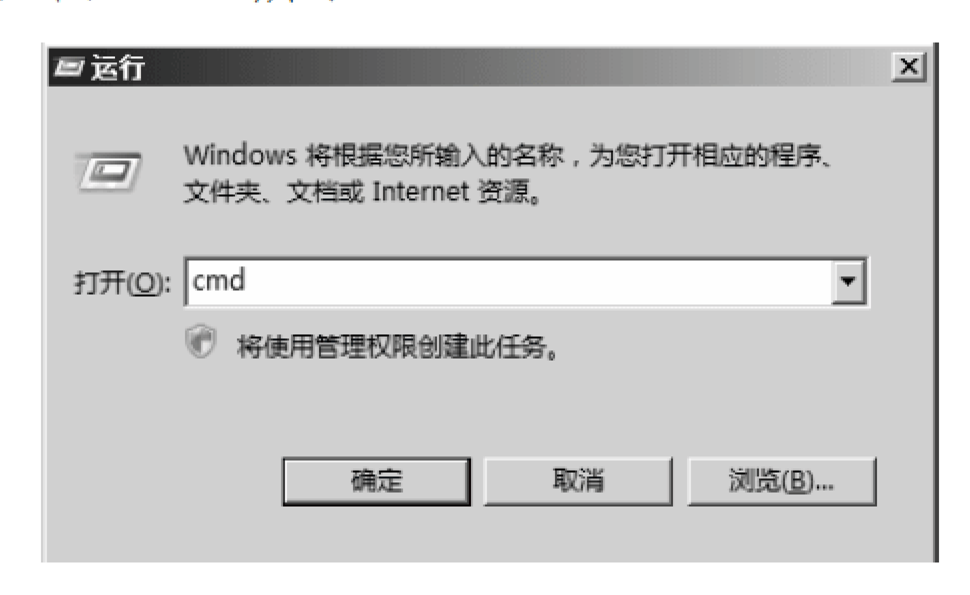


图 11-21

02 弹出【命令提示符】对话框，输入“netstat –an”命令，按【Enter】键确认，则可以看到操作系统正在进行的通信连接情况，如图 11-22 所示。

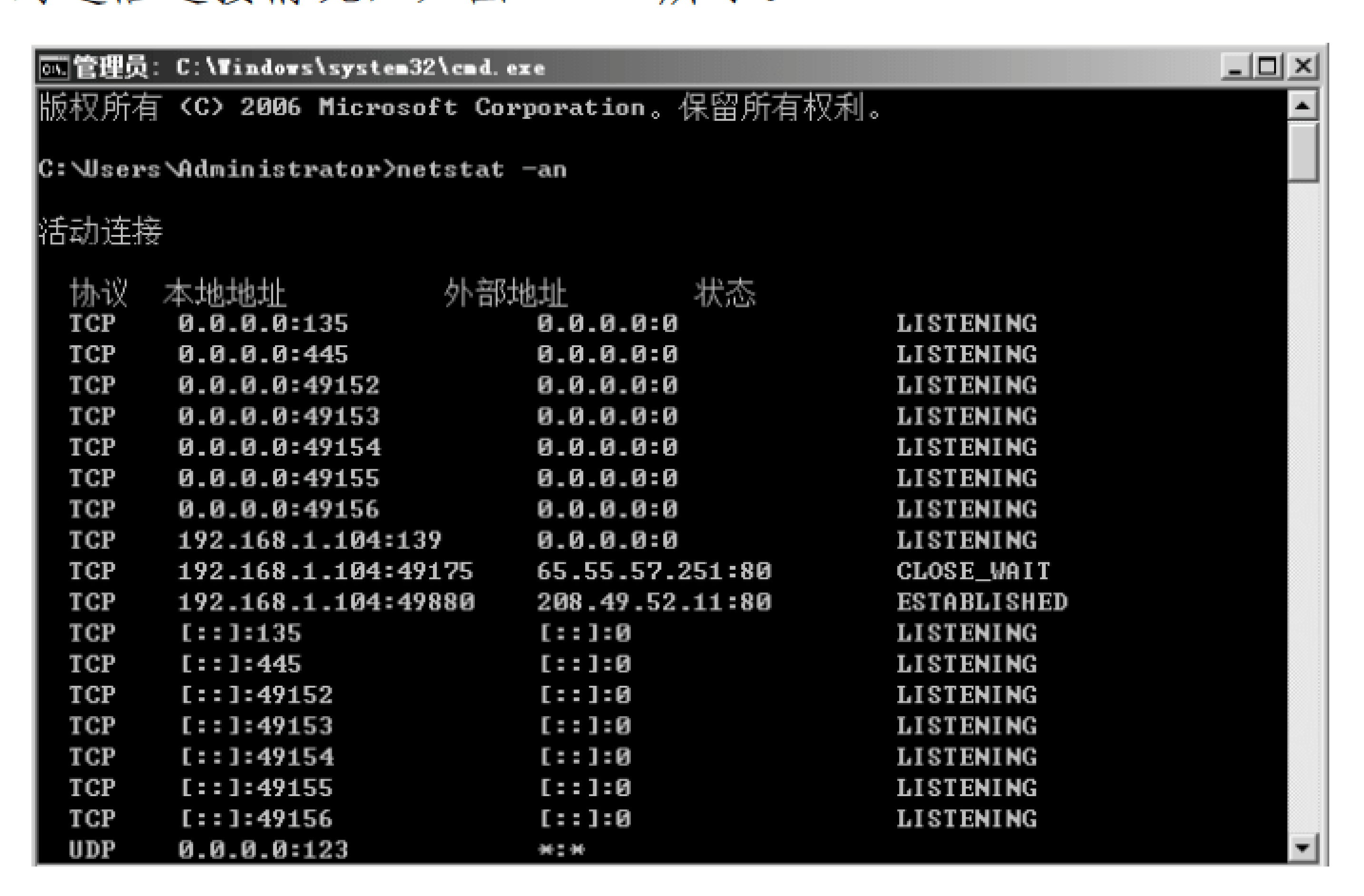


图 11-22

①本地地址是指操作系统正在用本地的哪个主机 IP 和端口与外界通信。

②外部地址是指操作系统正在与外部的哪个主机 IP 和端口进行通信。

2. 查看本机进程的端口占用情况

查看本机的什么进程占用哪个端口的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“cmd”命令，单击【确定】按钮，如图 11-23 所示。

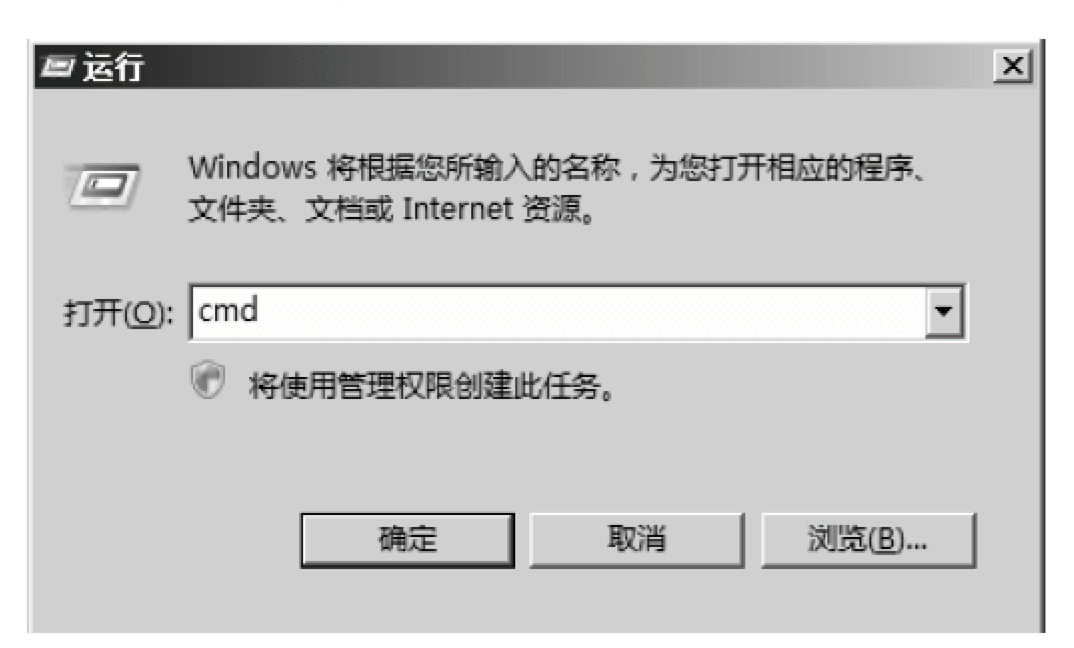


图 11-23

02 弹出【命令提示符】对话框，输入“netstat –bn”命令，按【Enter】键，则可以看到操作系统的哪个进程占用了哪个端口，如图 11-24 所示。

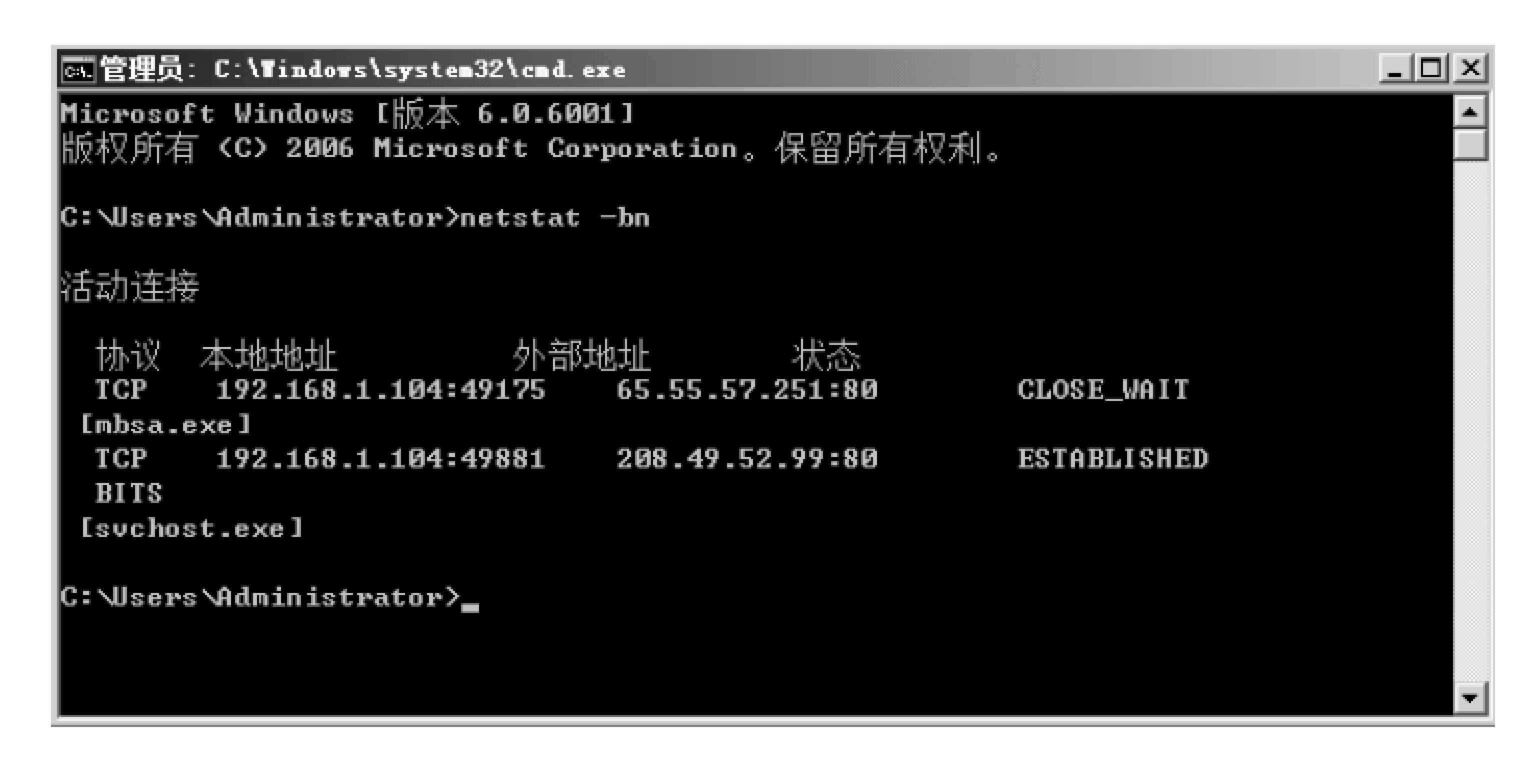


图 11-24

11.2.2 配置端口

通过运行端口查看命令，可以发现系统很多端口都是默认开启的，这就为服务器的安全留下了隐患，必须将可能存在安全风险的端口及时关闭。比如常见的 TCP 端口 135、139 和 1025，UDP 端口 123、137、138 等。

1. 关闭服务法

网络服务需要和外界进行通信，这时就需要用到端口，有时候一个网络服务需要一个端口，比如 FTP 服务需要 21 端口，因此要想关闭 21 端口，只需要将 FTP 服务器关掉即可。有时候一个网络服务却需要多个端口。

以关闭 FTP 服务为例，关闭端口的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“services.msc”命令，单击【确定】按钮，如图 11-25 所示。

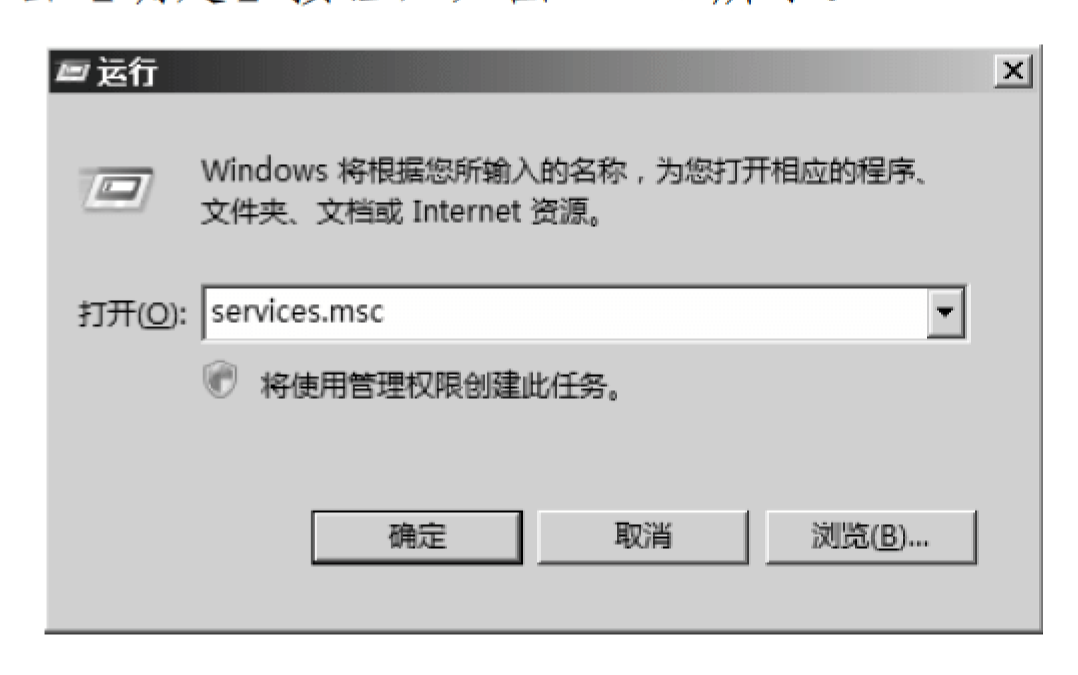


图 11-25

02 弹出【服务】窗口，找到【FTP Publishing Services】服务，如图 11-26 所示。

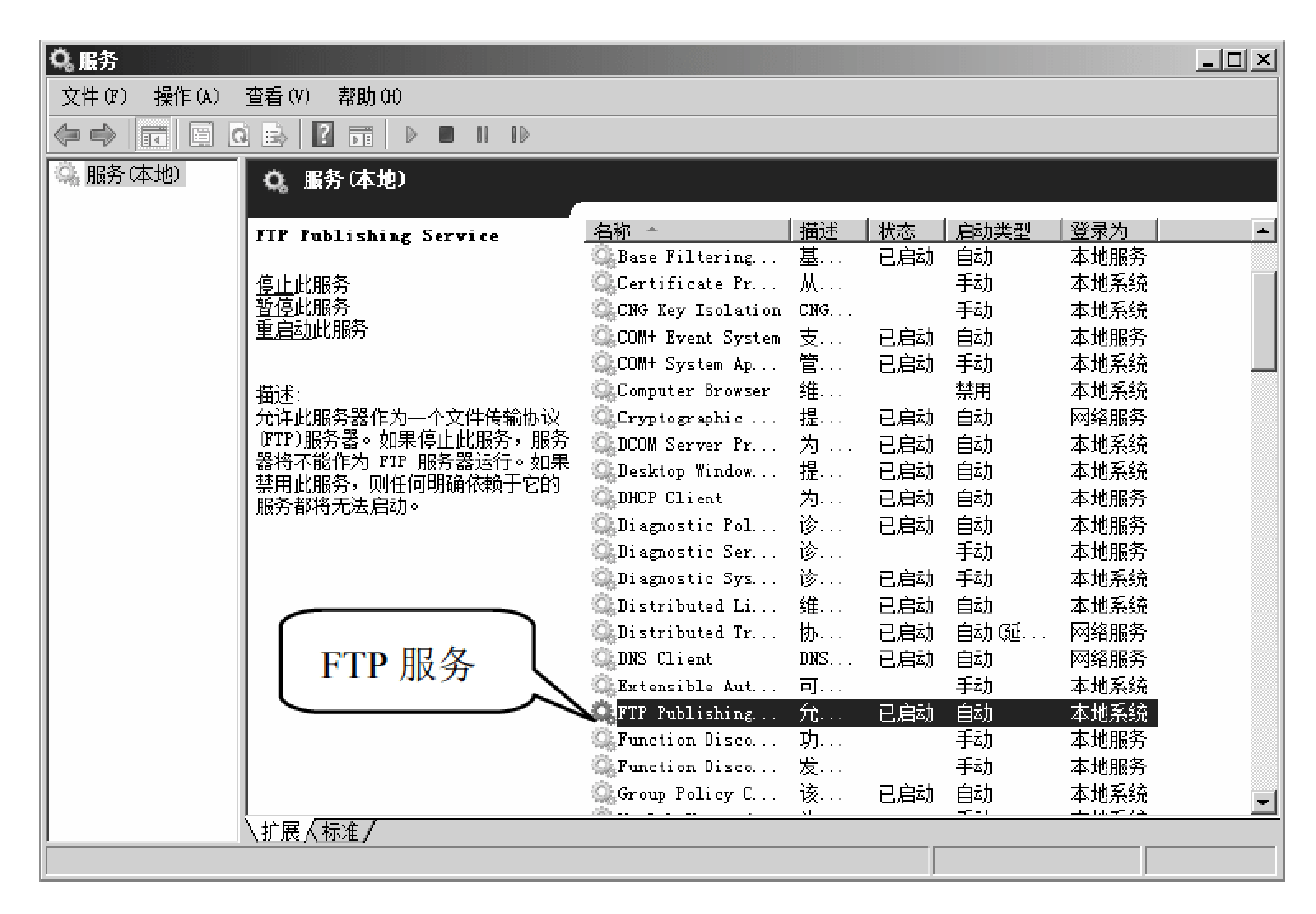


图 11-26

03 右击【FTP Publishing Services】服务，在弹出的快捷菜单中选择【属性】菜单命令，如图 11-27 所示。



图 11-27

04 弹出【FTP Publishing Service 属性】对话框，在【启动类型】下拉列表中选择【禁用】选项，单击【停止】按钮，然后单击【确定】按钮，如图 11-28 所示。FTP 服务已经关闭，FTP 服务所使用的 21 端口也被自动关闭。



图 11-28

2. IP 安全策略法

利用 IP 策略可以关闭服务器不需要开启的端口或者只开启服务器需要开启的端口，从而达到保证服务器安全的目的。本实例通过介绍不允许访问服务器的 139 端口为例，来介绍如何使用 IP 安全策略关闭端口，具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“gpedit.msc”命令，单击【确定】按钮，如图 11-29 所示。

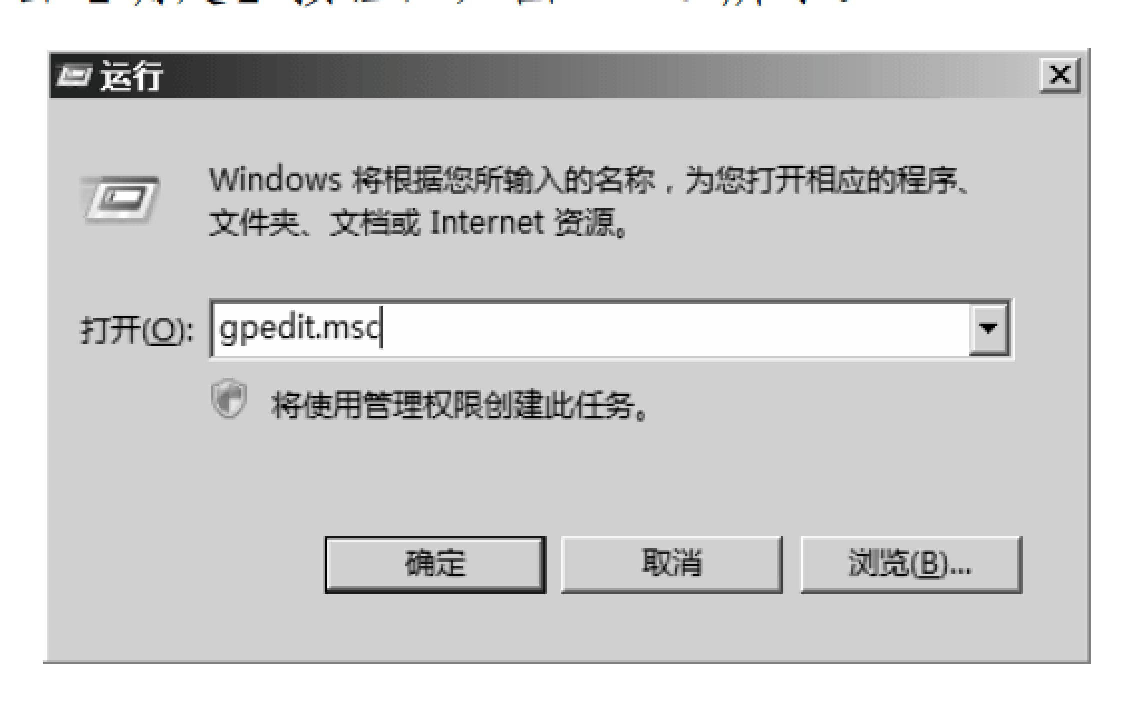


图 11-29

02 弹出【本地组策略编辑器】窗口，在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【IP 安全策略】选项，如图 11-30 所示。

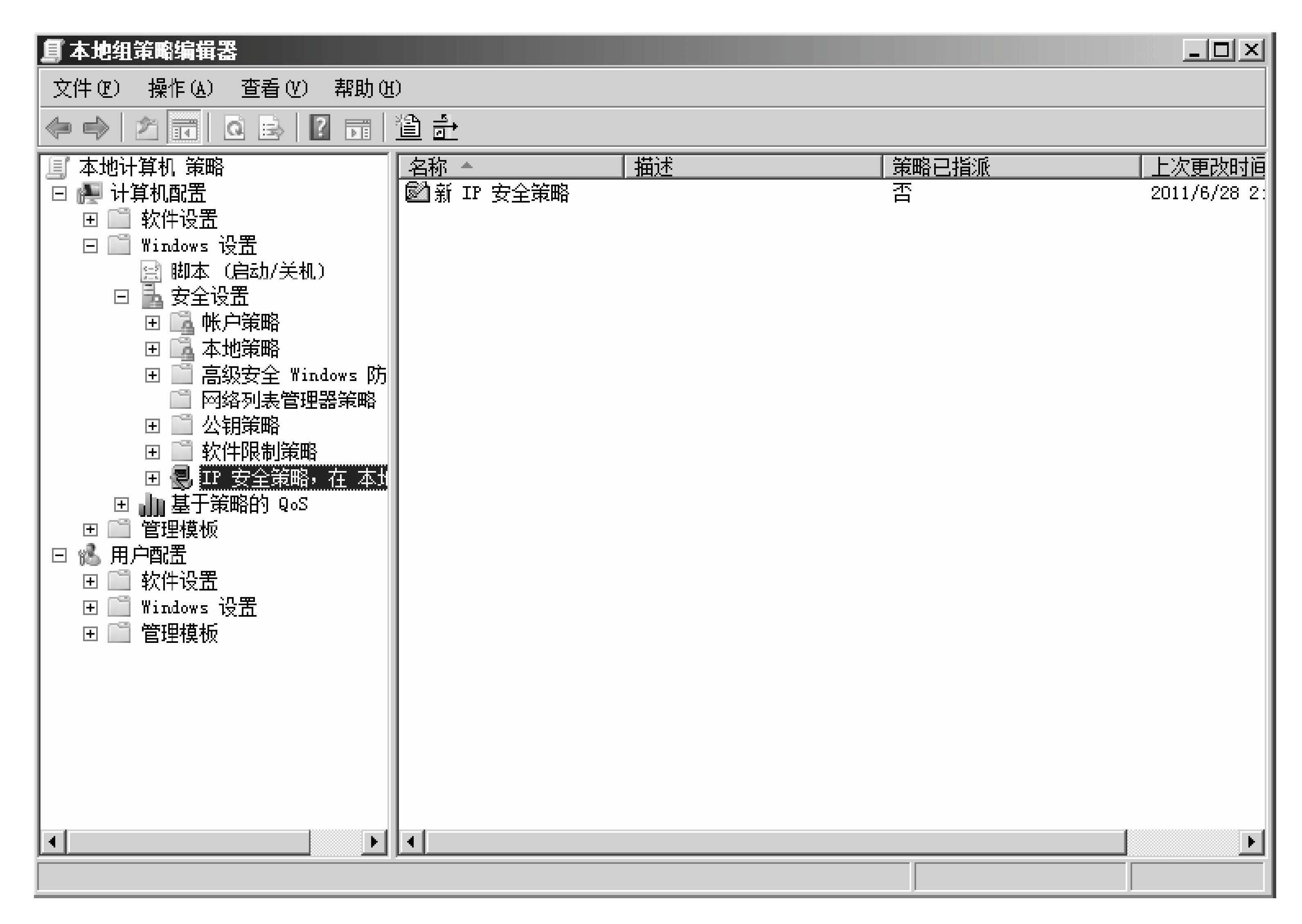


图 11-30

03 右击【IP 安全策略】选项，在弹出的快捷菜单中选择【创建 IP 安全策略】菜单命令，如图 11-31 所示。



图 11-31

04 弹出【IP 安全策略向导】对话框，单击【下一步】按钮，如图 11-32 所示。

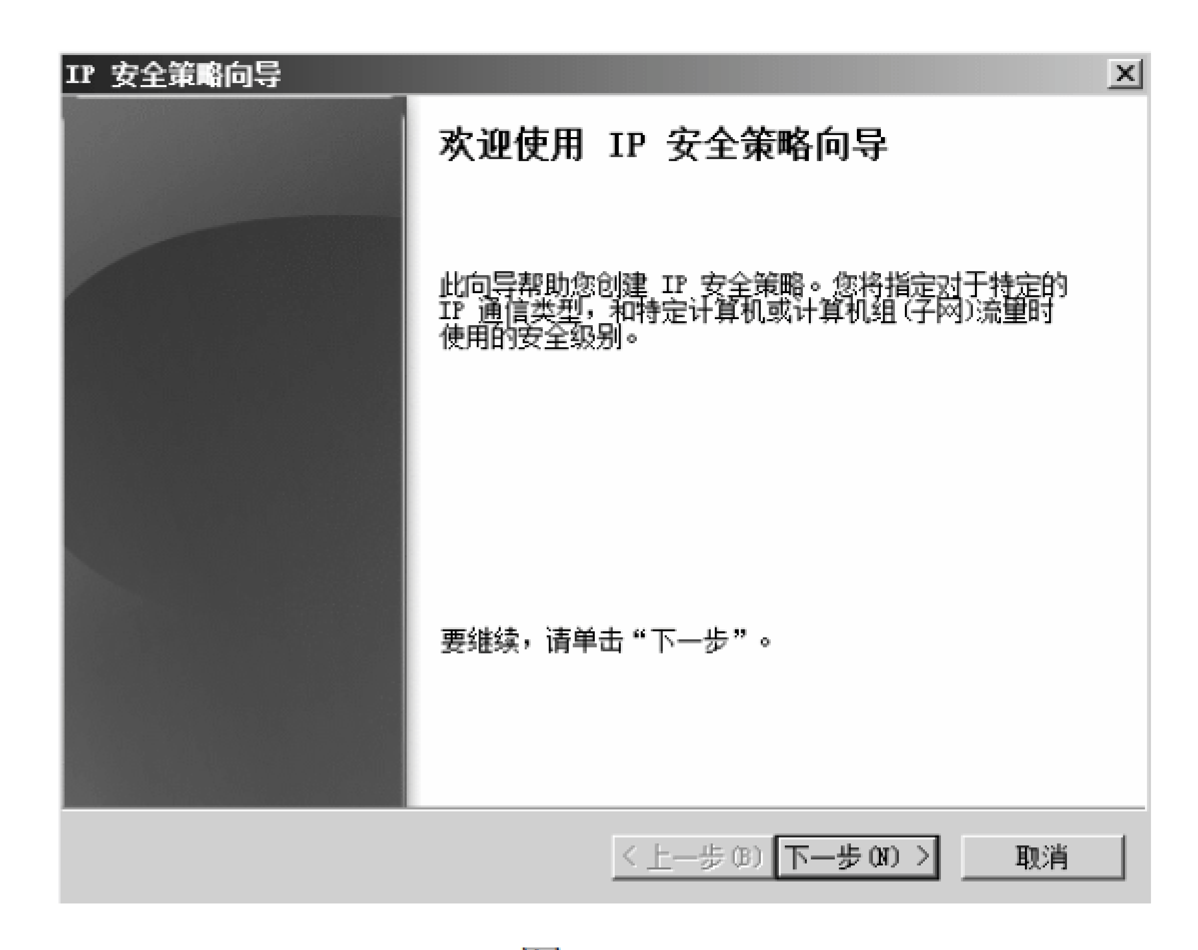


图 11-32

05 弹出【IP 安全策略名称】对话框，在【名称】文本框中输入名称“禁用 139 端口”，单击【下一步】按钮，如图 11-33 所示。

图 11-33

06 弹出【安全通讯请求】对话框，单击【下一步】按钮，如图 11-34 所示。

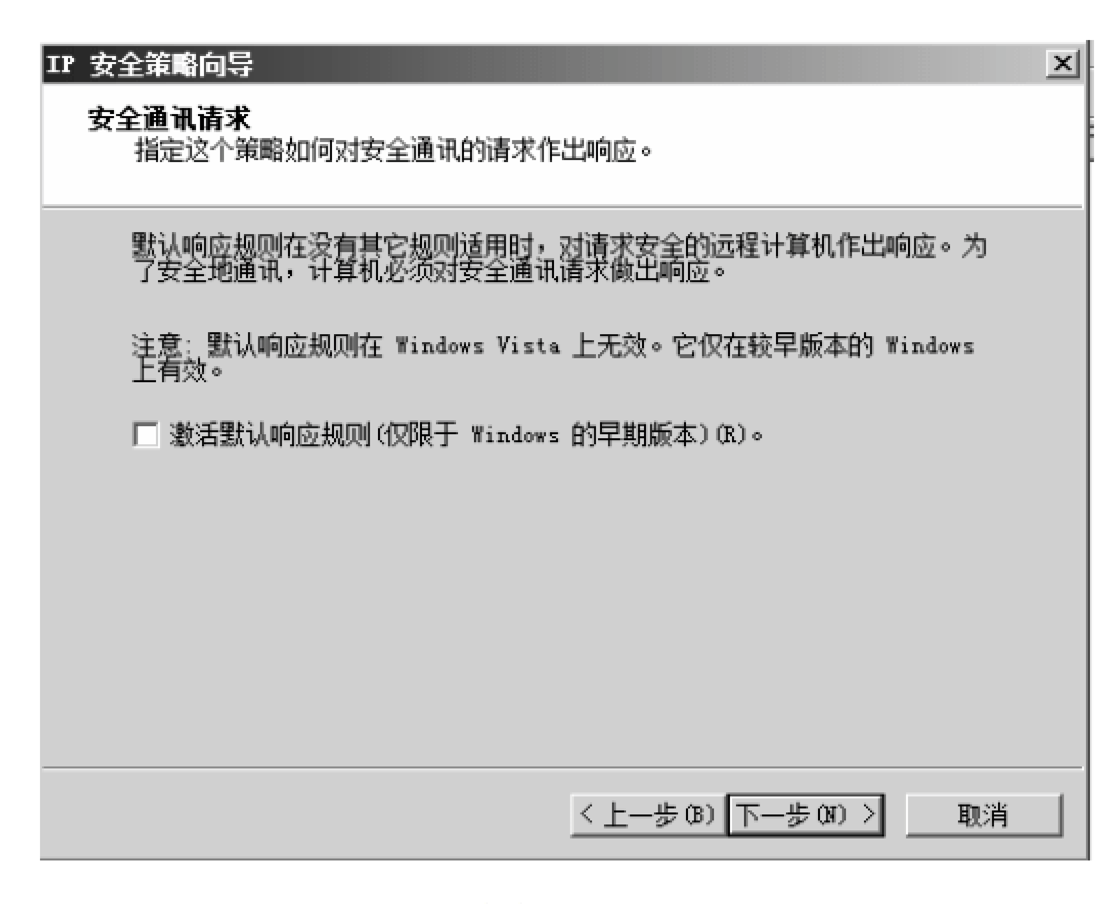


图 11-34

07 弹出【正在完成 IP 安全策略向导】对话框，选择【编辑属性】单选框，单击【完成】按钮，如图 11-35 所示。

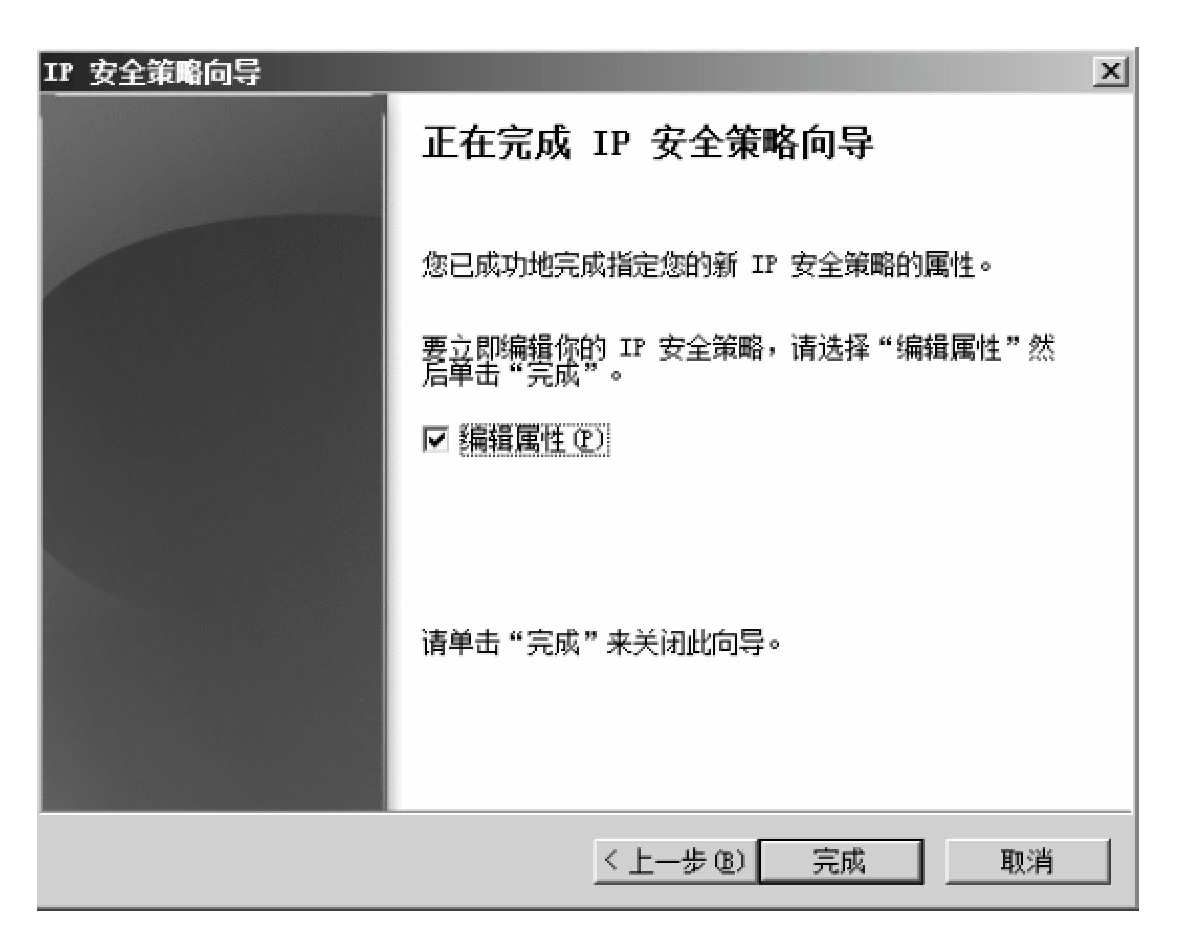


图 11-35

08 弹出【禁用 139 端口属性】对话框，单击【添加】按钮，如图 11-36 所示。



图 11-36

09 弹出【安全规则向导】对话框，单击【下一步】按钮，如图 11-37 所示。

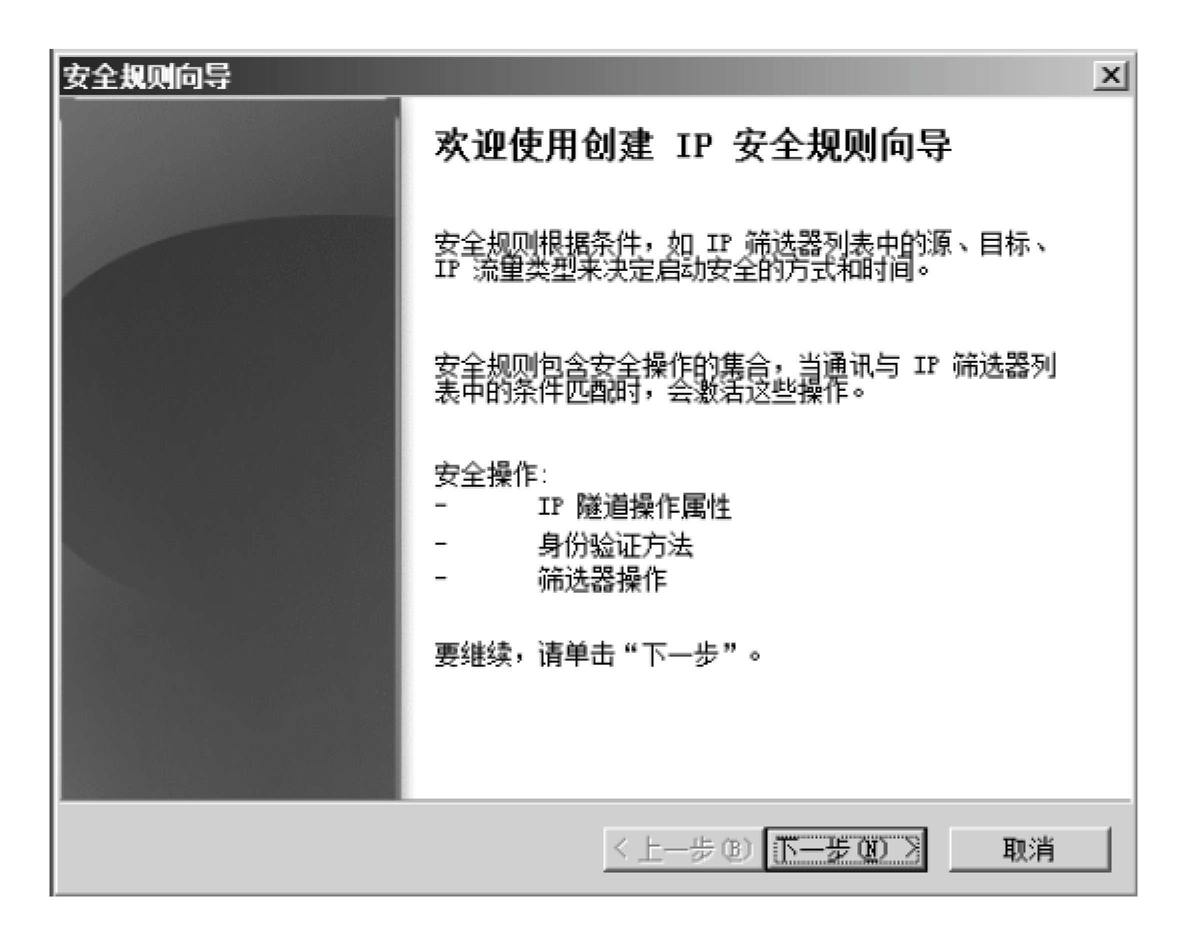


图 11-37

10 弹出【隧道终结点】对话框，选择【此规则不指定隧道】单选按钮，单击【下一步】按钮，如图 11-38 所示。

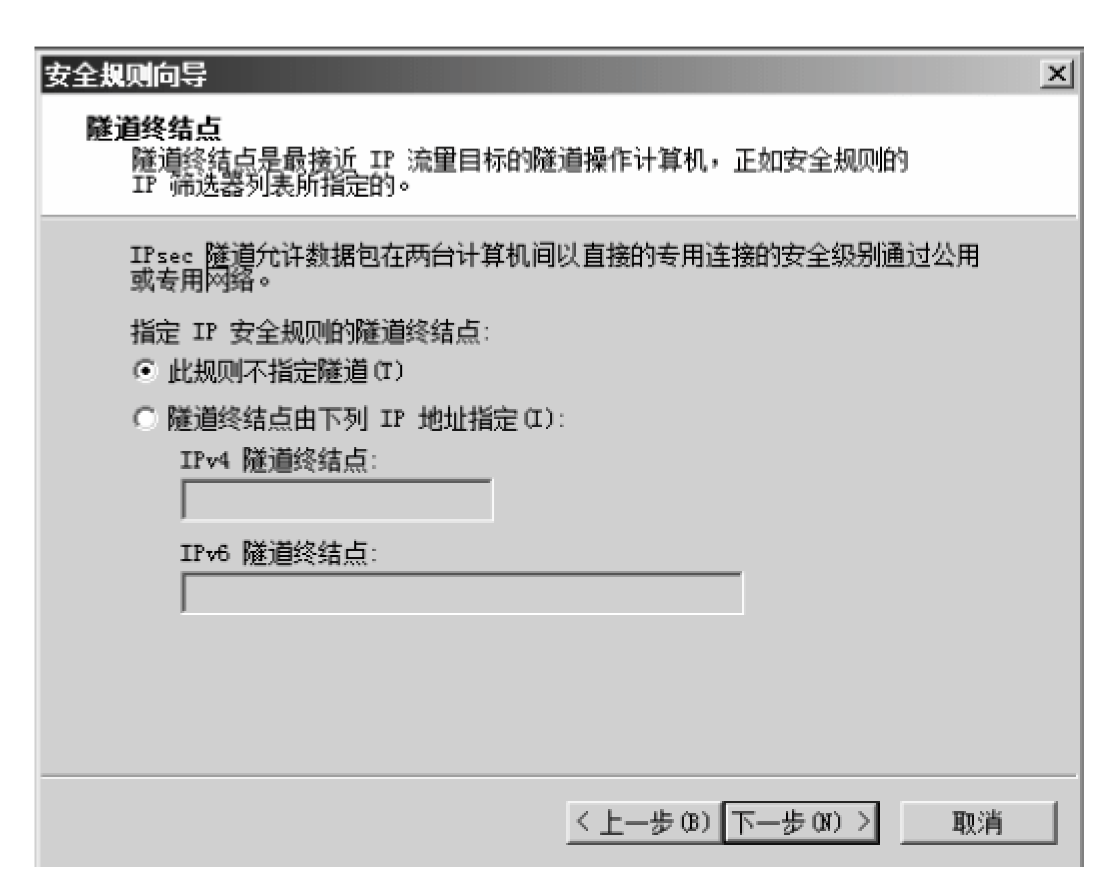


图 11-38

11 弹出【网络类型】对话框，选择【所有网络连接】单选按钮，单击【下一步】按钮，如图 11-39 所示。

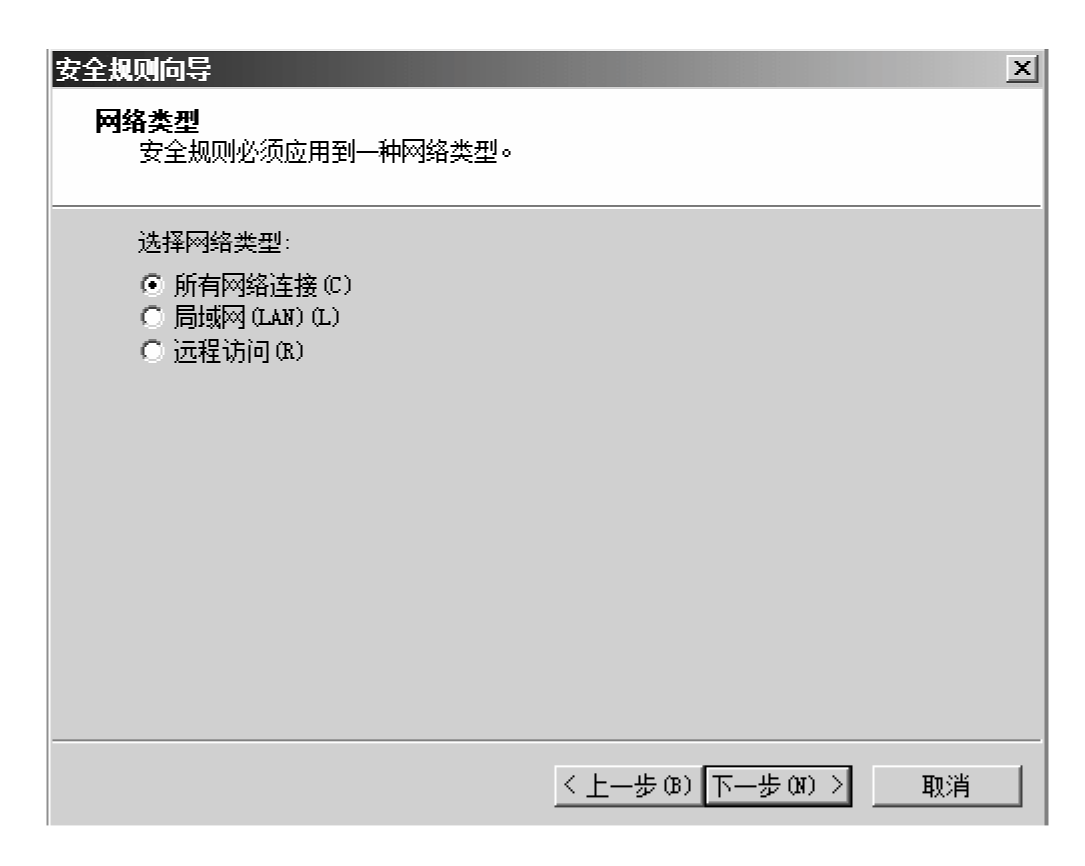


图 11-39

12 弹出【IP 筛选器列表】对话框，单击【下一步】按钮，如图 11-40 所示。

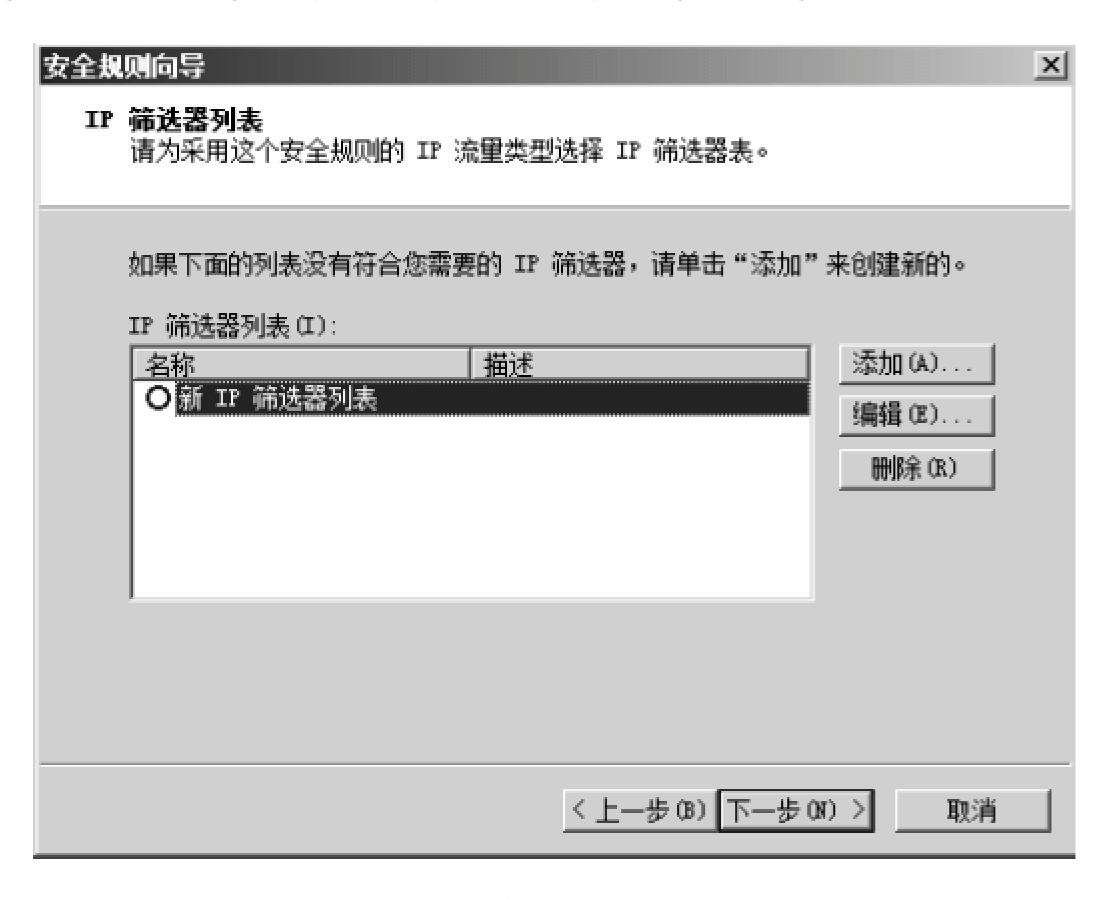


图 11-40

13 弹出【IP 筛选器列表】对话框，在【名称】文本框中输入 IP 筛选器列表的名称为"禁止 139 端口通信"，选择【使用添加向导】复选框，单击【添加】按钮，如图 11-41 所示。

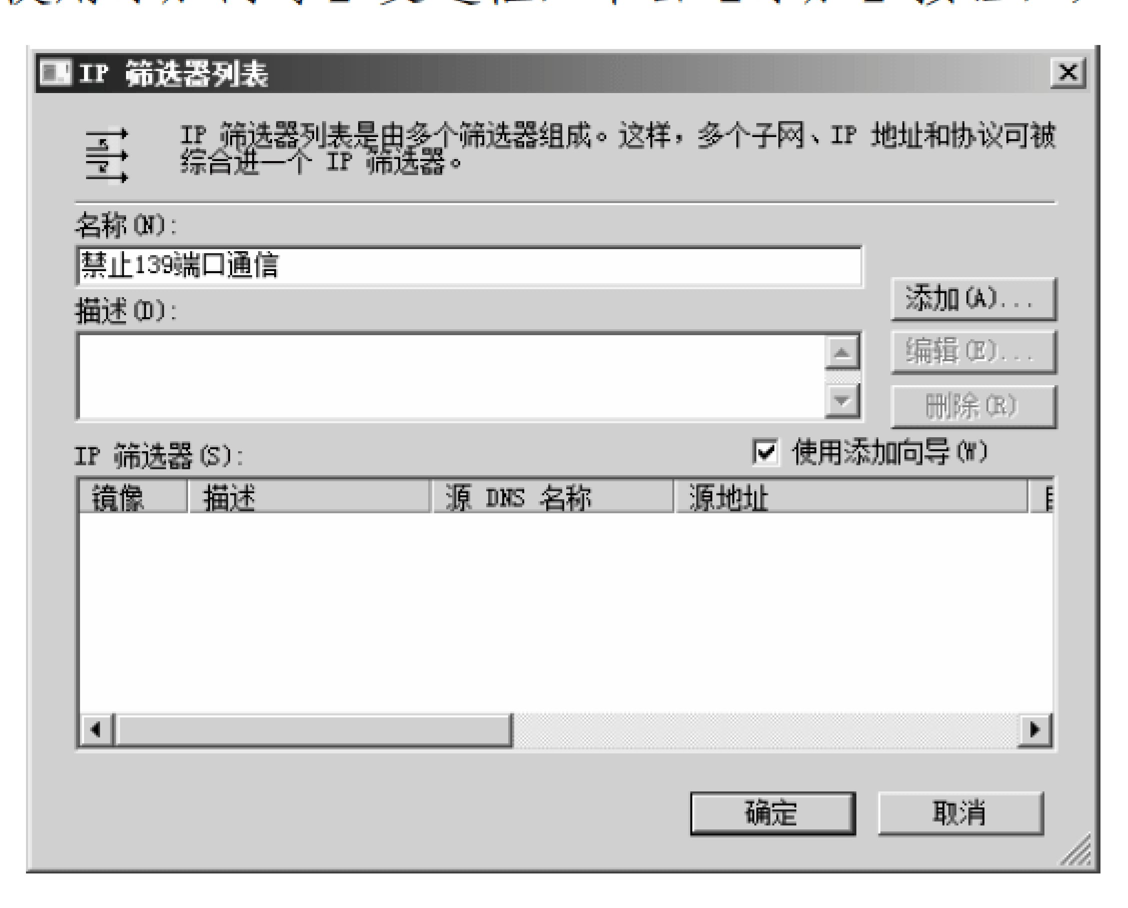


图 11-41

14 弹出【IP 筛选器向导】对话框，单击【下一步】按钮，如图 11-42 所示。

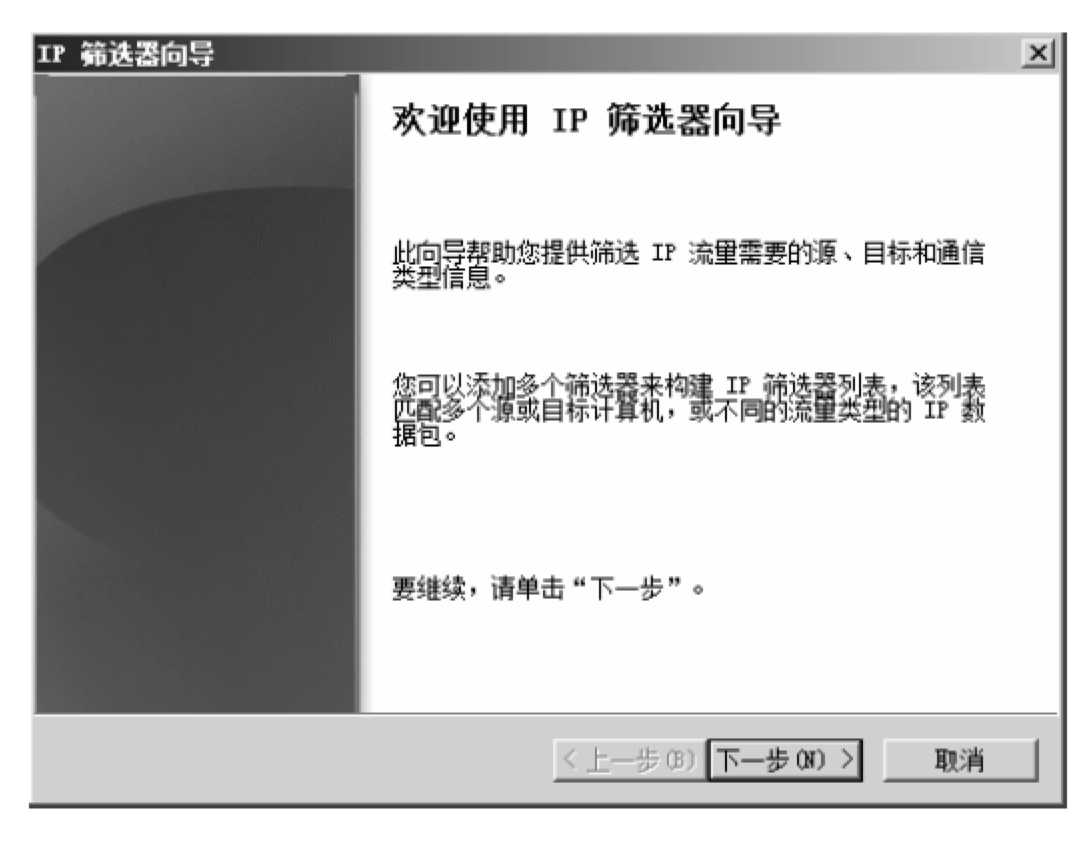


图 11-42

15 弹出【IP 筛选器描述和镜像属性】对话框，在【描述】文本框中输入描述信息“禁止 139 端口通信”，选择【镜像】复选框，单击【下一步】按钮，如图 11-43 所示。

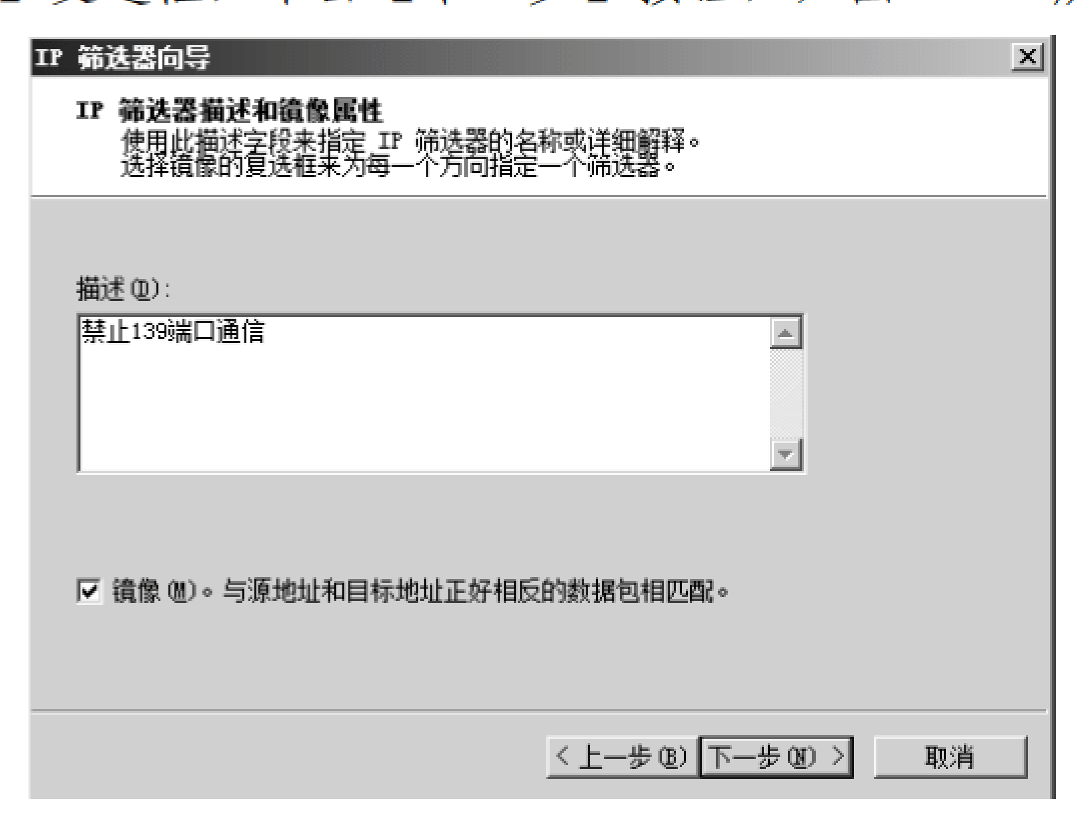


图 11-43

16 弹出【IP 流量源】对话框，在【源地址】下拉菜单中选择【任何 IP 地址】选项，单击【下一步】按钮，如图 11-44 所示。



图 11-44

17 弹出【IP 流量目标】对话框，在【目标地址】下拉列表中选择【我的 IP 地址】选项，如图 11-45 所示，单击【下一步】按钮。

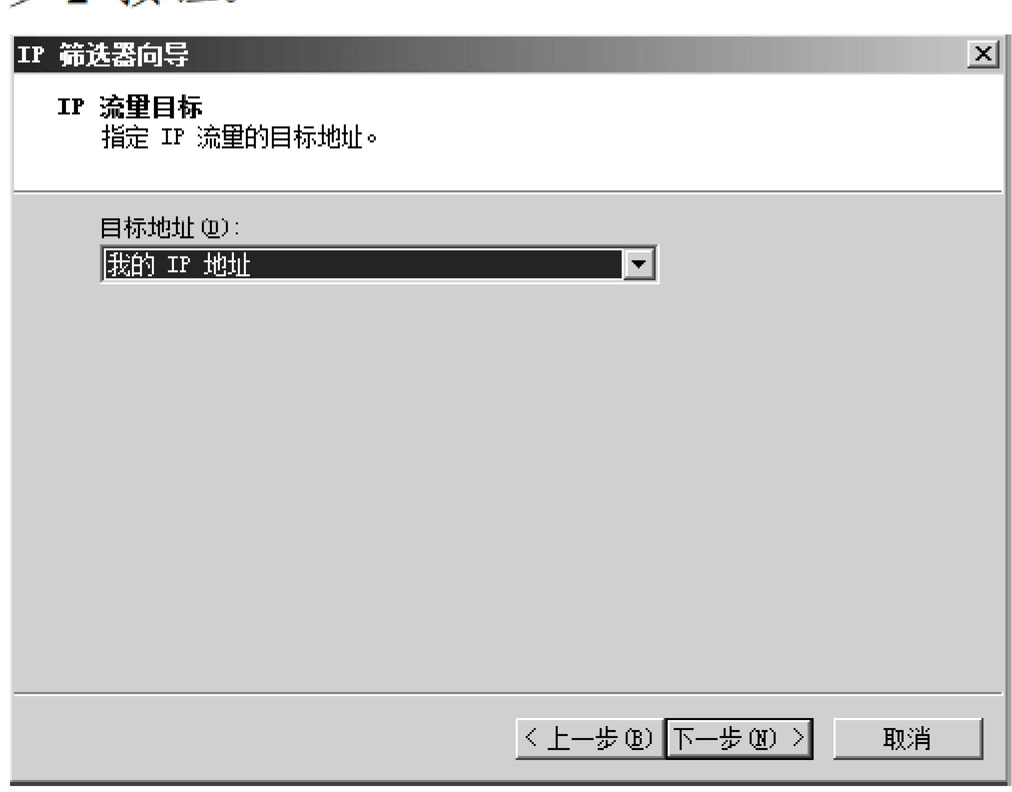


图 11-45

18 弹出【IP 协议类型】对话框，在【选择协议类型】下拉列表中选择【TCP】选项，如图 11-46 所示，单击【下一步】按钮。

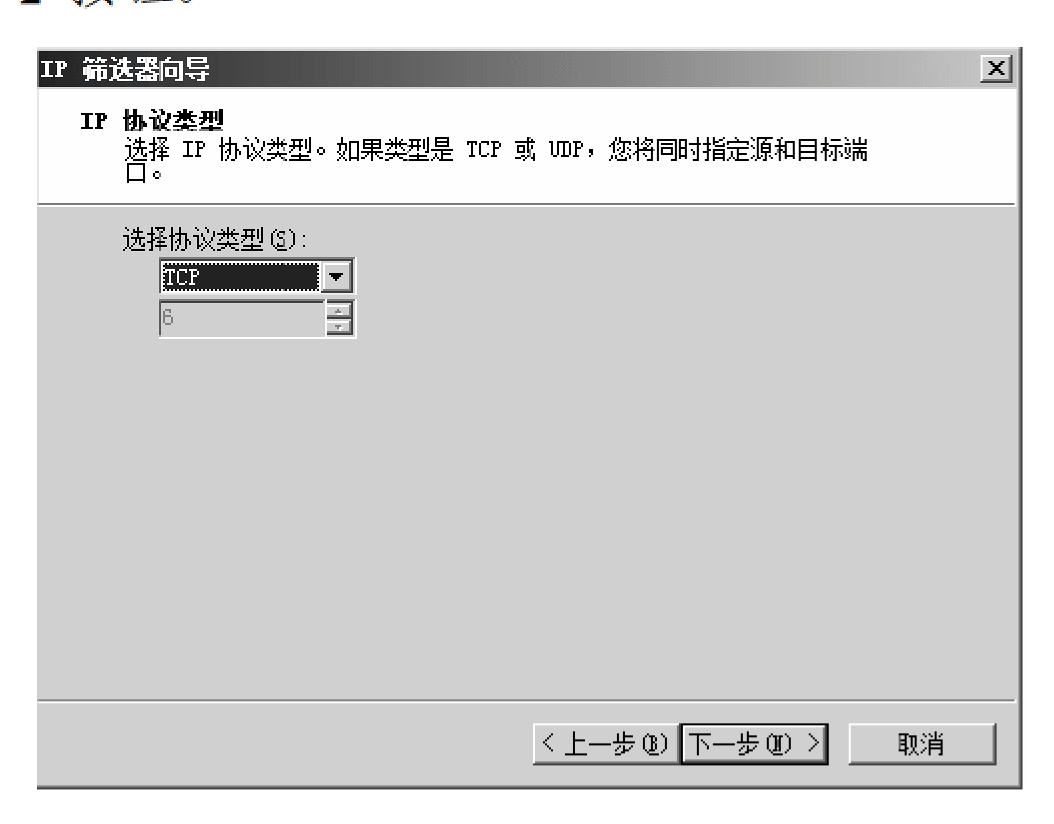


图 11-46

19 弹出【IP 协议端口】对话框，选择【从任意端口】和【到此端口】单选按钮，在【到此端口】文本框中输入“139”，表明数据包的目的端口为 139，如图 11-47 所示，单击【下一步】按钮。

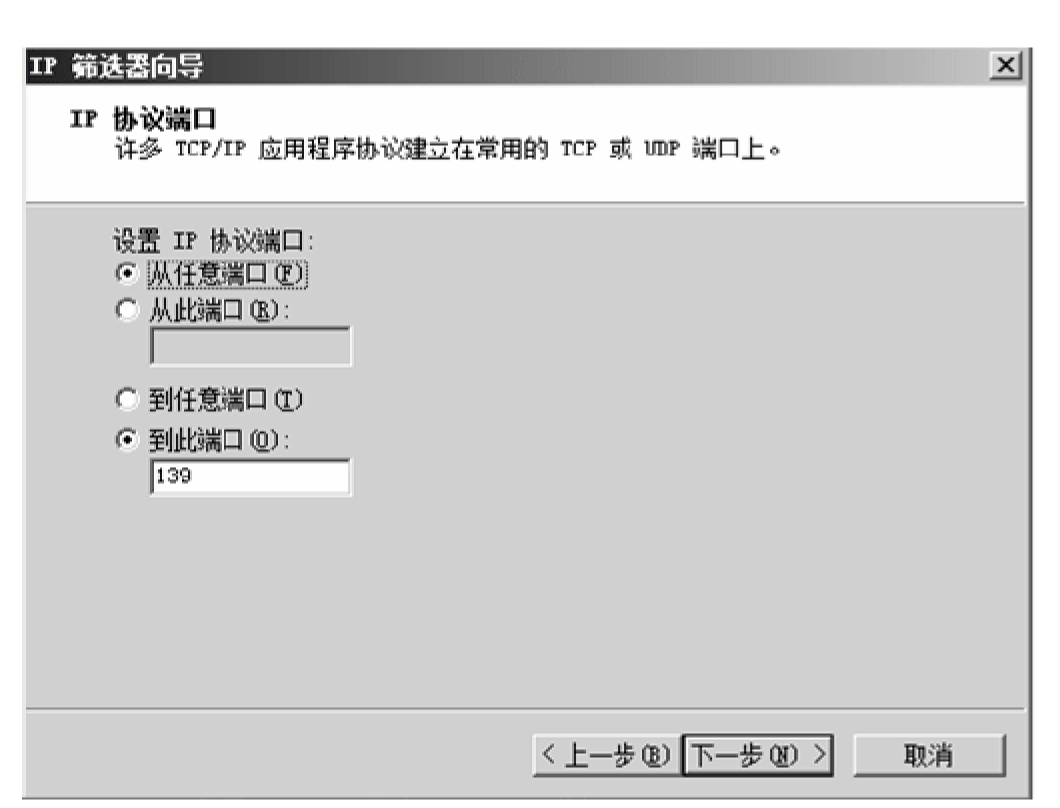


图 11-47

20 弹出【正在完成 IP 筛选器向导】对话框，单击【完成】按钮，如图 11-48 所示。

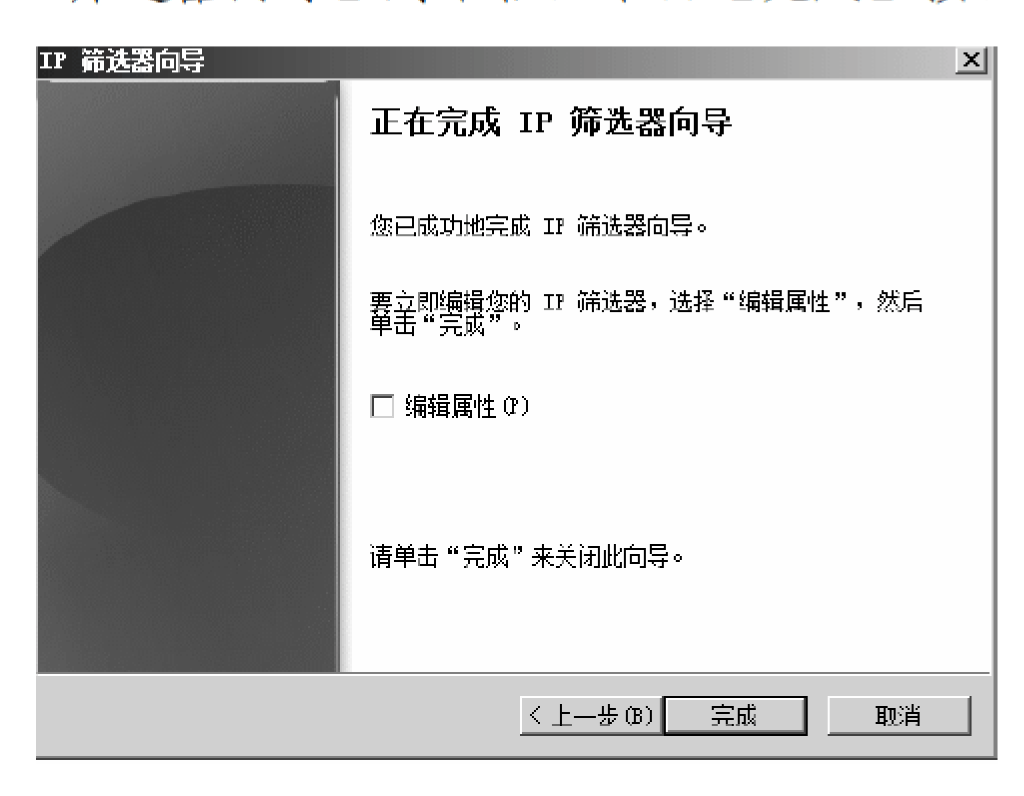


图 11-48

21 返回【IP 筛选器列表】对话框，单击【确定】按钮，如图 11-49 所示。

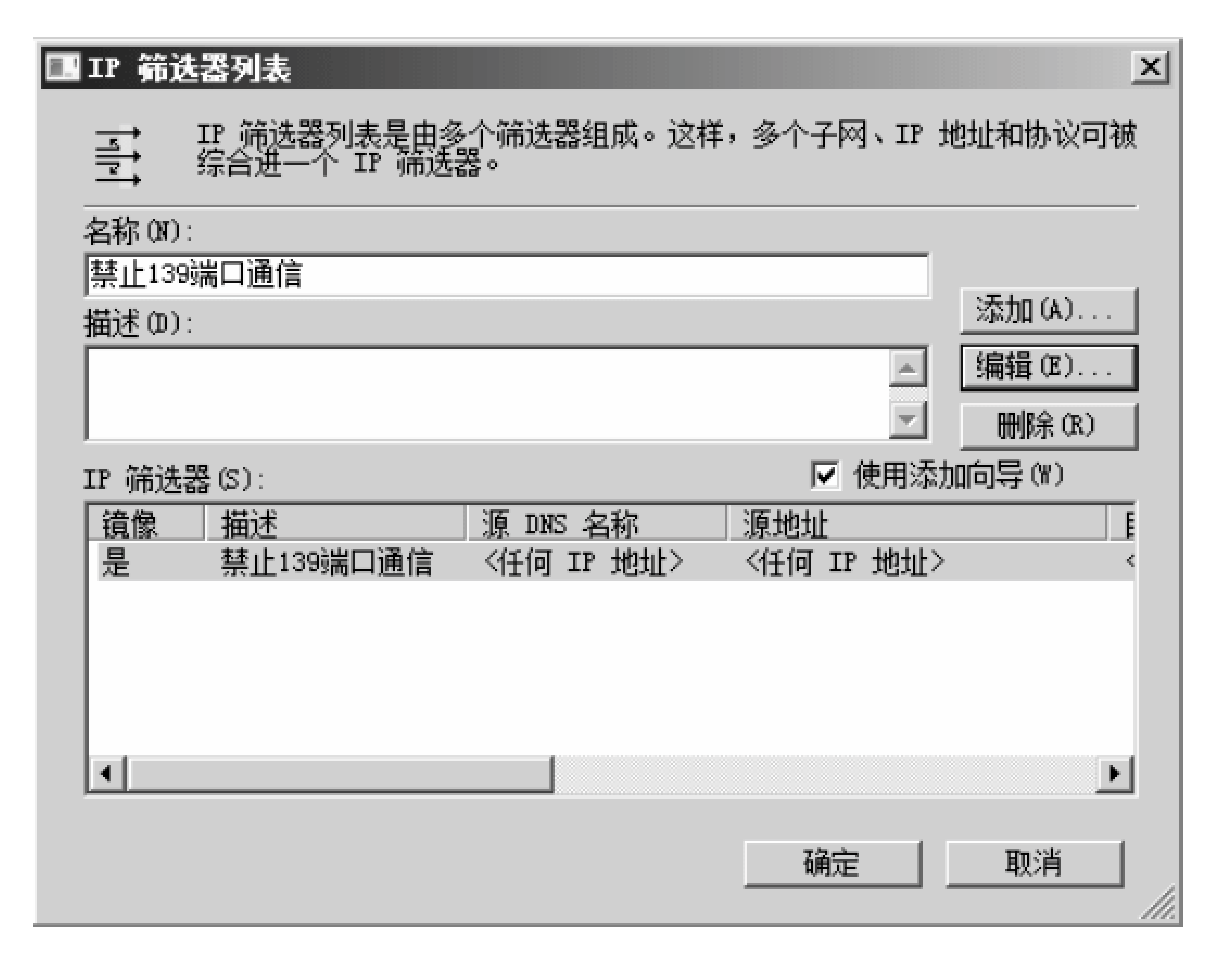


图 11-49

22 返回【新规则属性】对话框，选择【禁止 139 端口通信】单选按钮，如图 11-50 所示，选择【筛选器操作】选项卡。

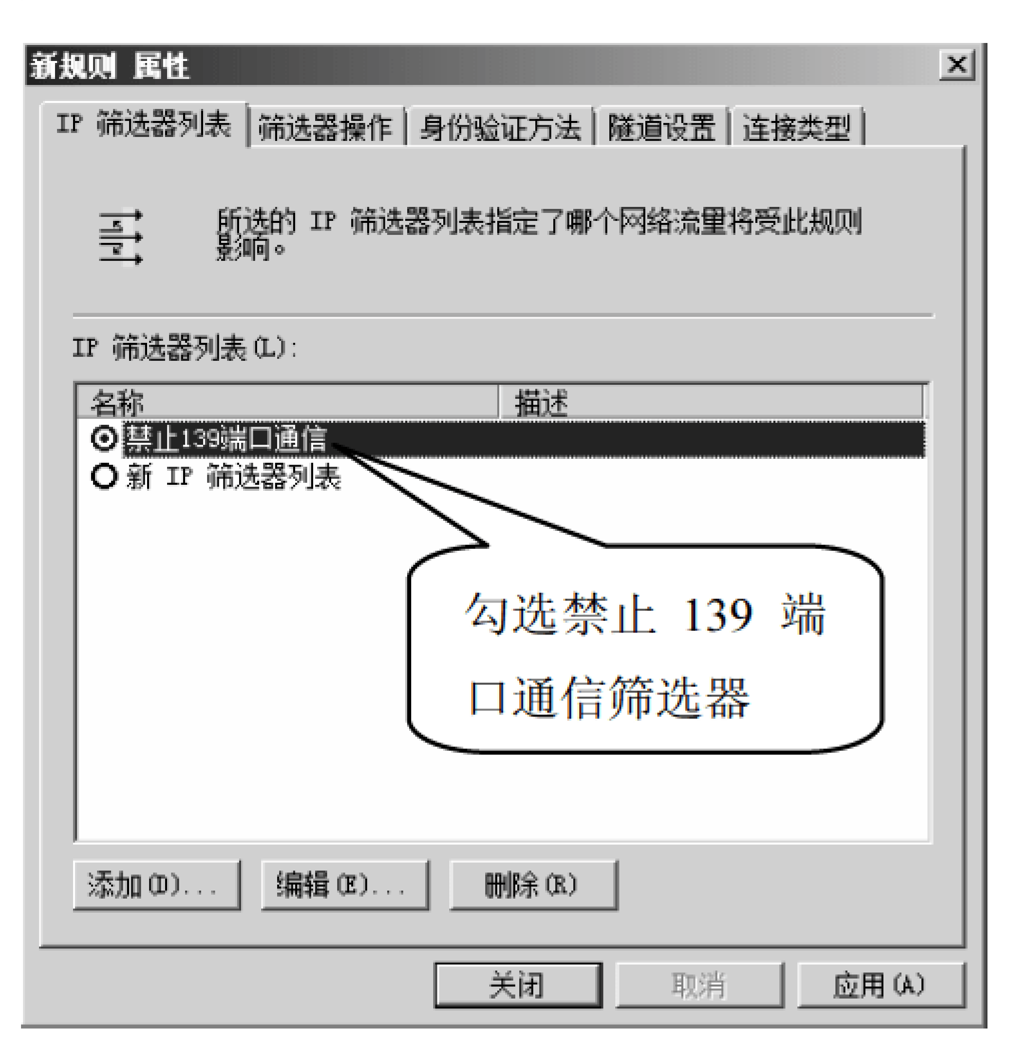


图 11-50

23 弹出【筛选器操作】对话框，单击【添加】按钮，如图 11-51 所示。

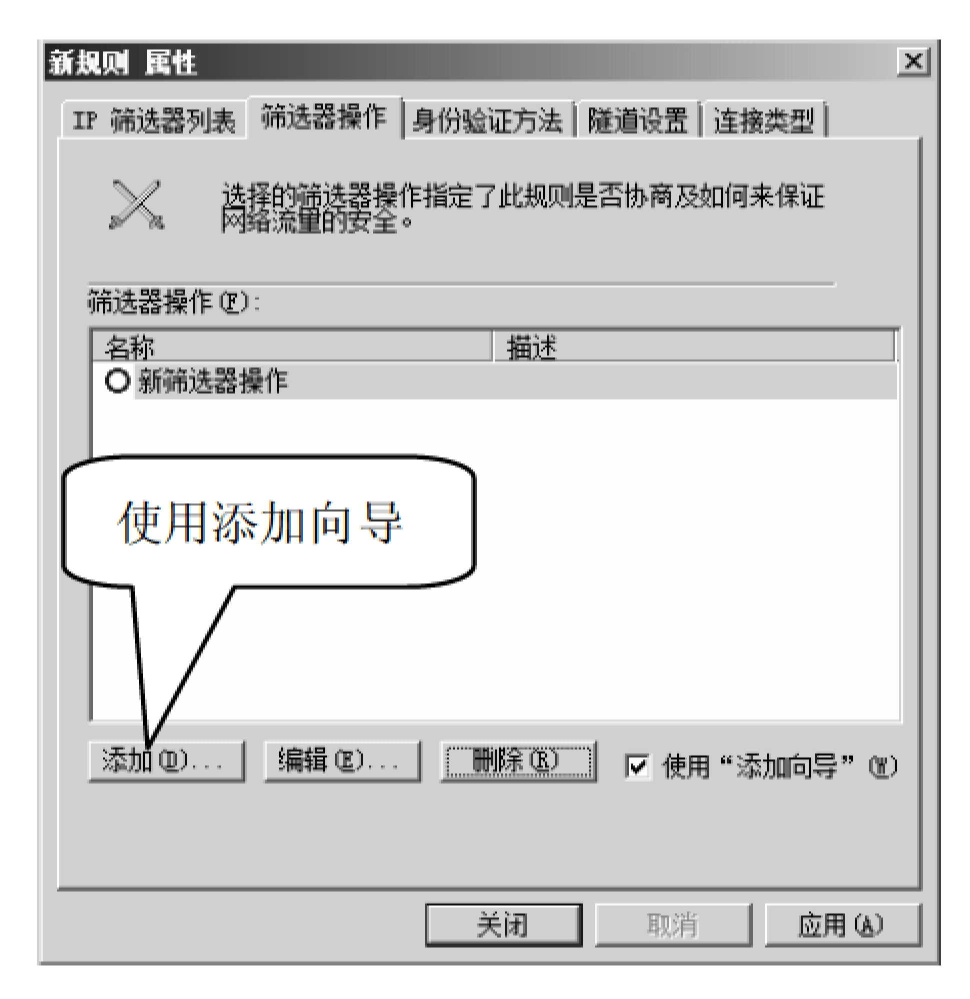


图 11-51

24 弹出【筛选器操作向导】对话框，单击【下一步】按钮，如图 11-52 所示。

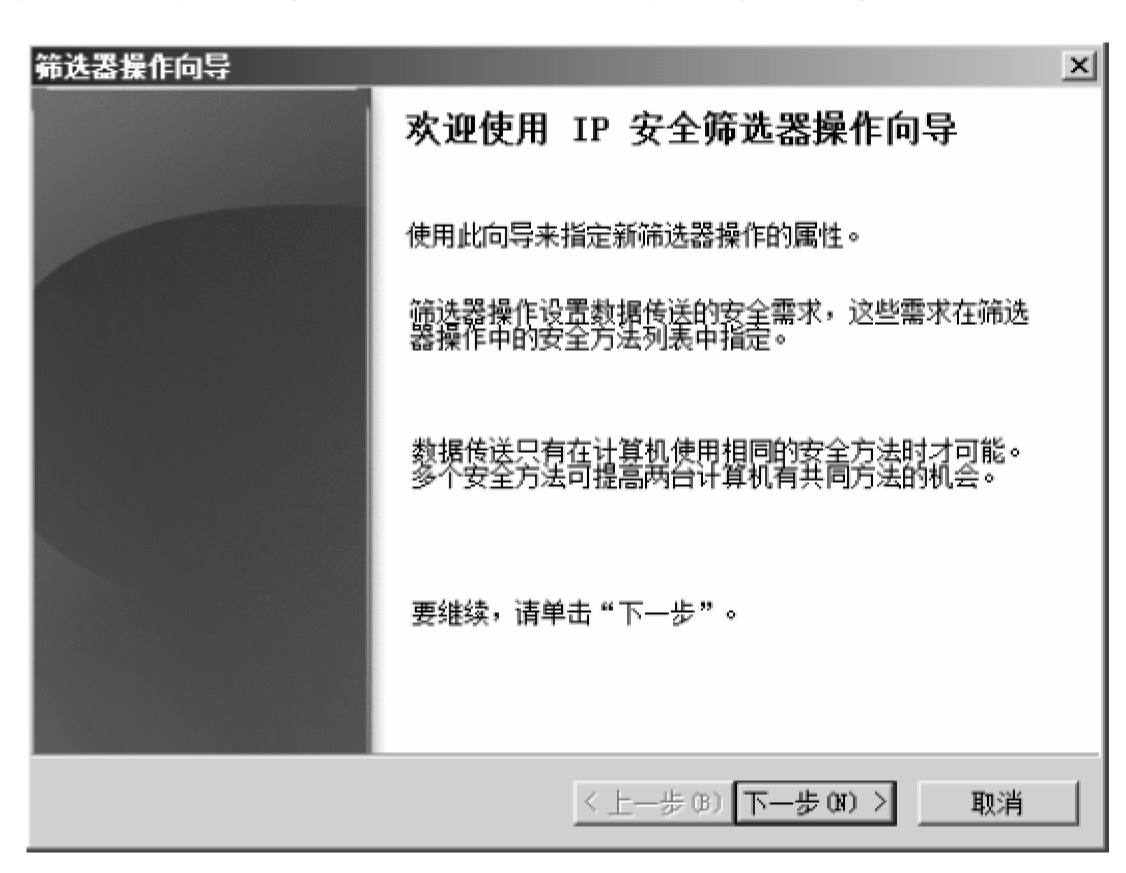


图 11-52

25 弹出【筛选器操作名称】对话框，在【名称】文本框中输入名称为“禁止通信” ，如图 11-53 所示，单击【下一步】按钮。

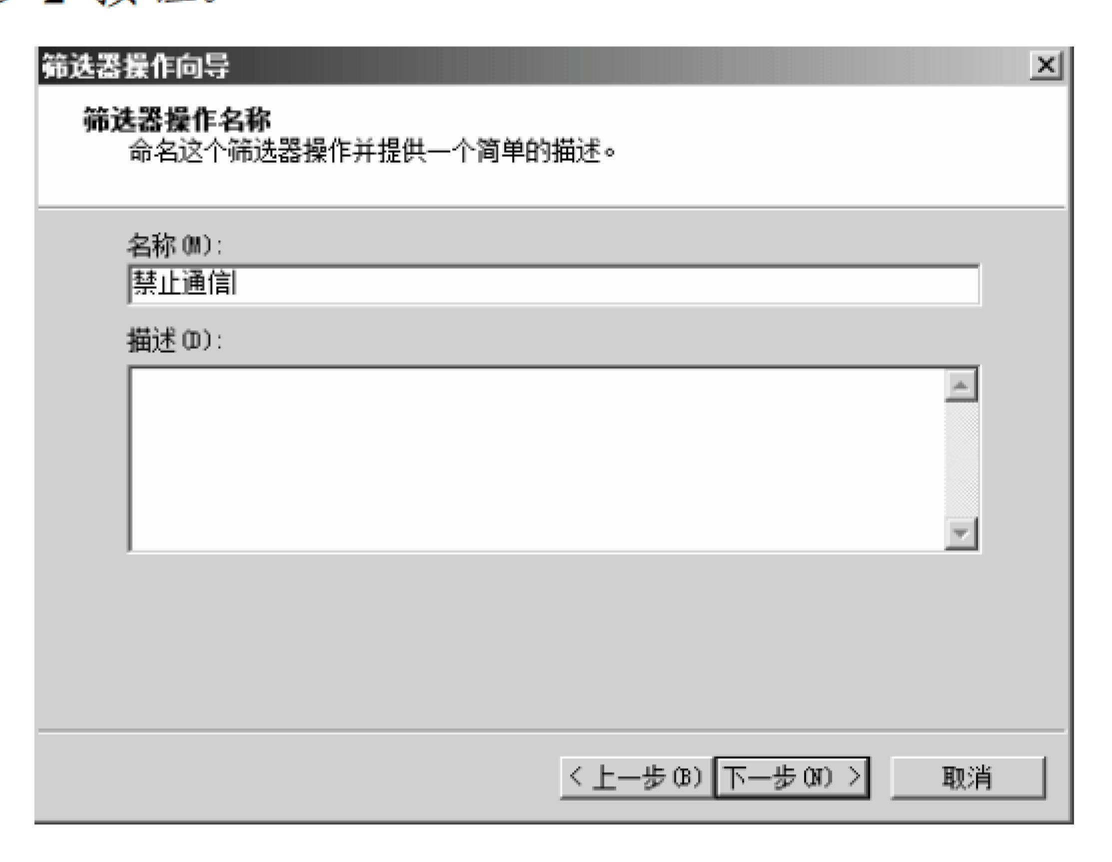


图 11-53

26 弹出【筛选器操作常规选项】对话框，选择【阻止】单选按钮，如图 11-54 所示，单击【下一步】按钮。



图 11-54

27 弹出【正在完成 IP 安全筛选器操作向导】对话框，单击【完成】按钮，如图 11-55 所示。

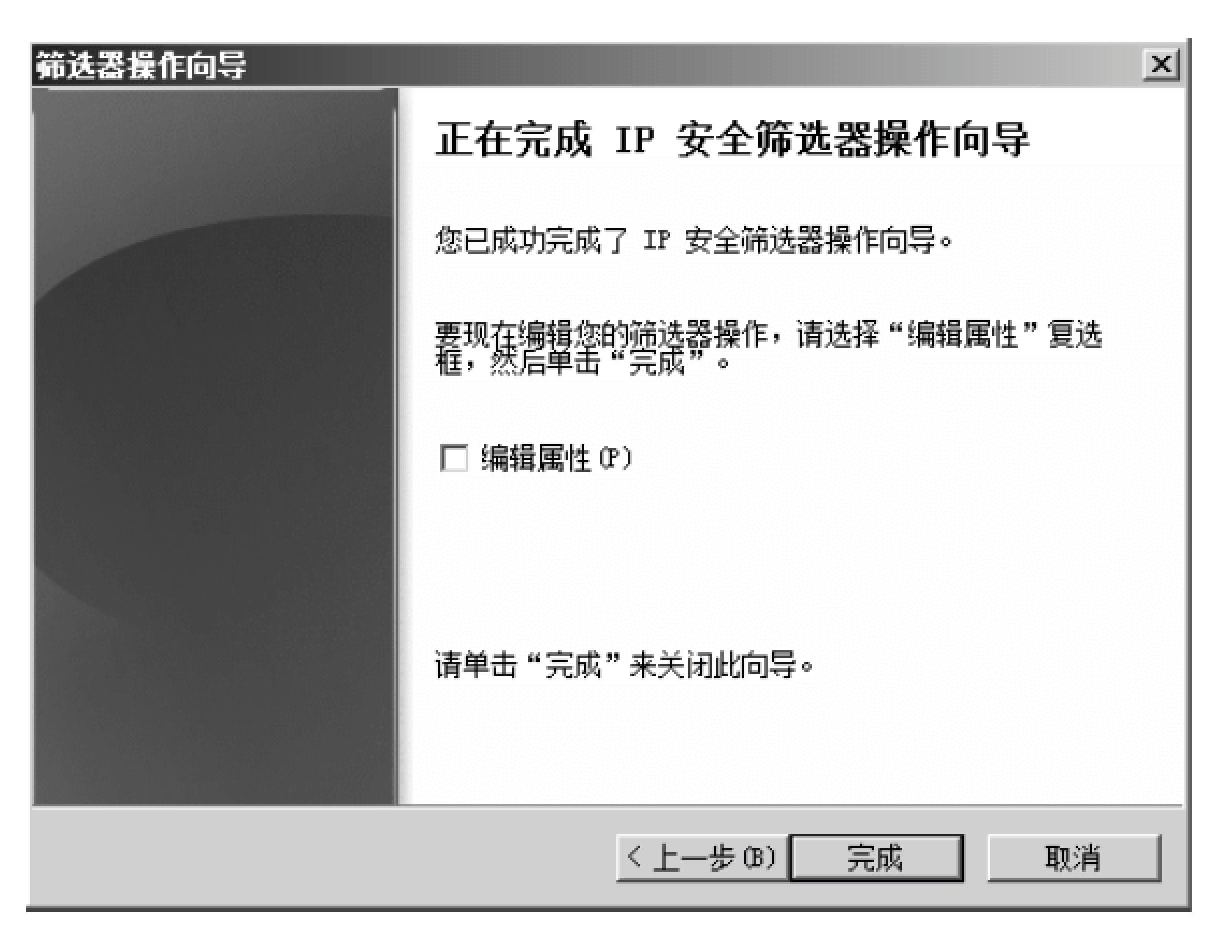


图 11-55

28 返回至【筛选器操作】对话框，选择【禁止通信】单选按钮，单击【应用】按钮，如图 11-56 所示，然后单击【关闭】按钮。

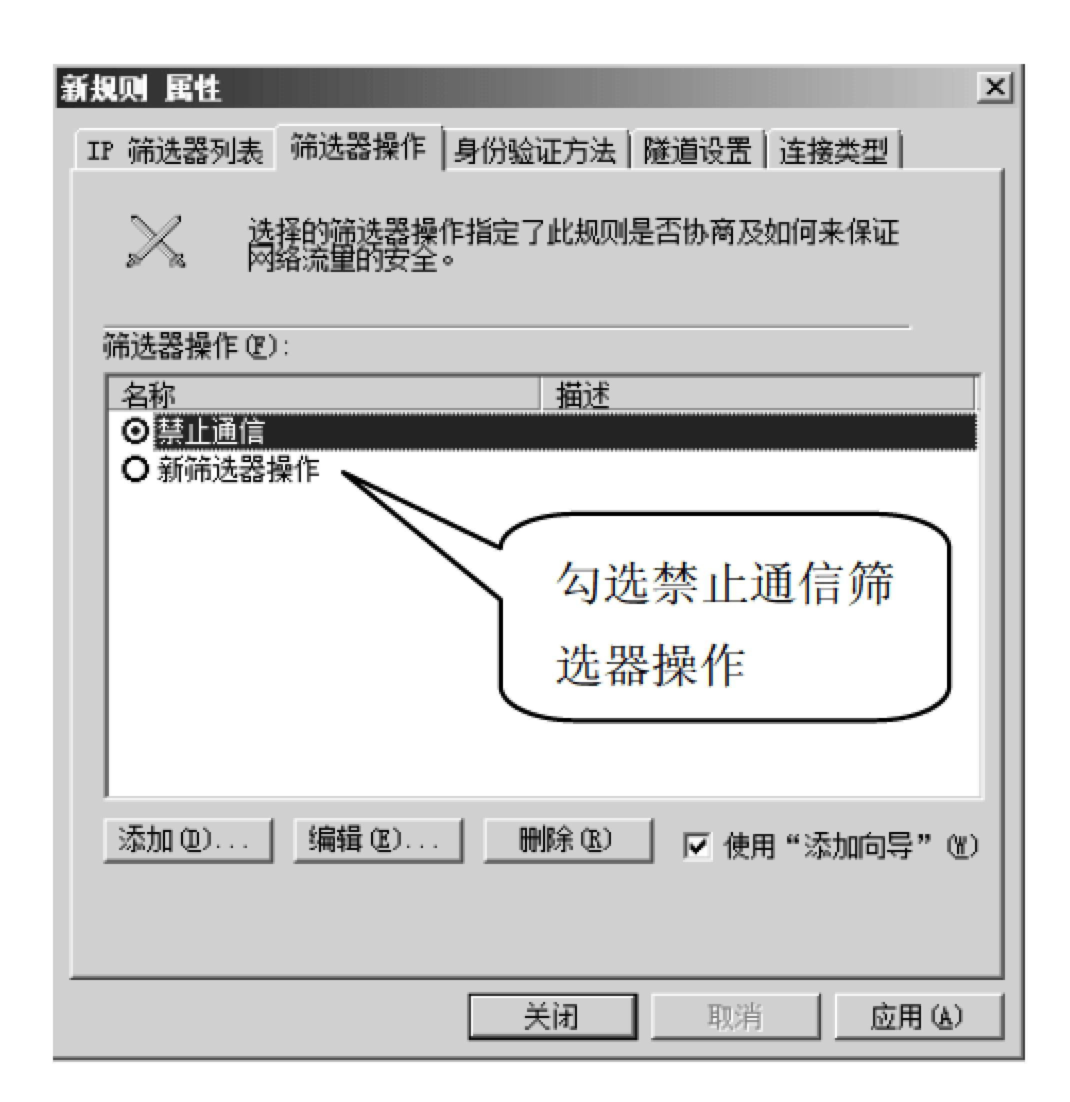


图 11-56

29 返回至【禁止 139 端口通信 属性】对话框，如图 11-57 所示，单击【确定】按钮。



图 11-57

30 返回至【本地组策略编辑器】窗口，右击【禁止 139 端口通信】策略，在弹出的快捷菜单中选择【所有任务】➢【分配】菜单命令，如图 11-58 所示。



图 11-58

31 如图 11-59 所示，至此【禁止 139 端口通信】安全策略已经被成功分配。现在所有的计算机都被禁止同本地计算机的 139 端口通信，也就意味着成功关闭了本机的 139 端口。

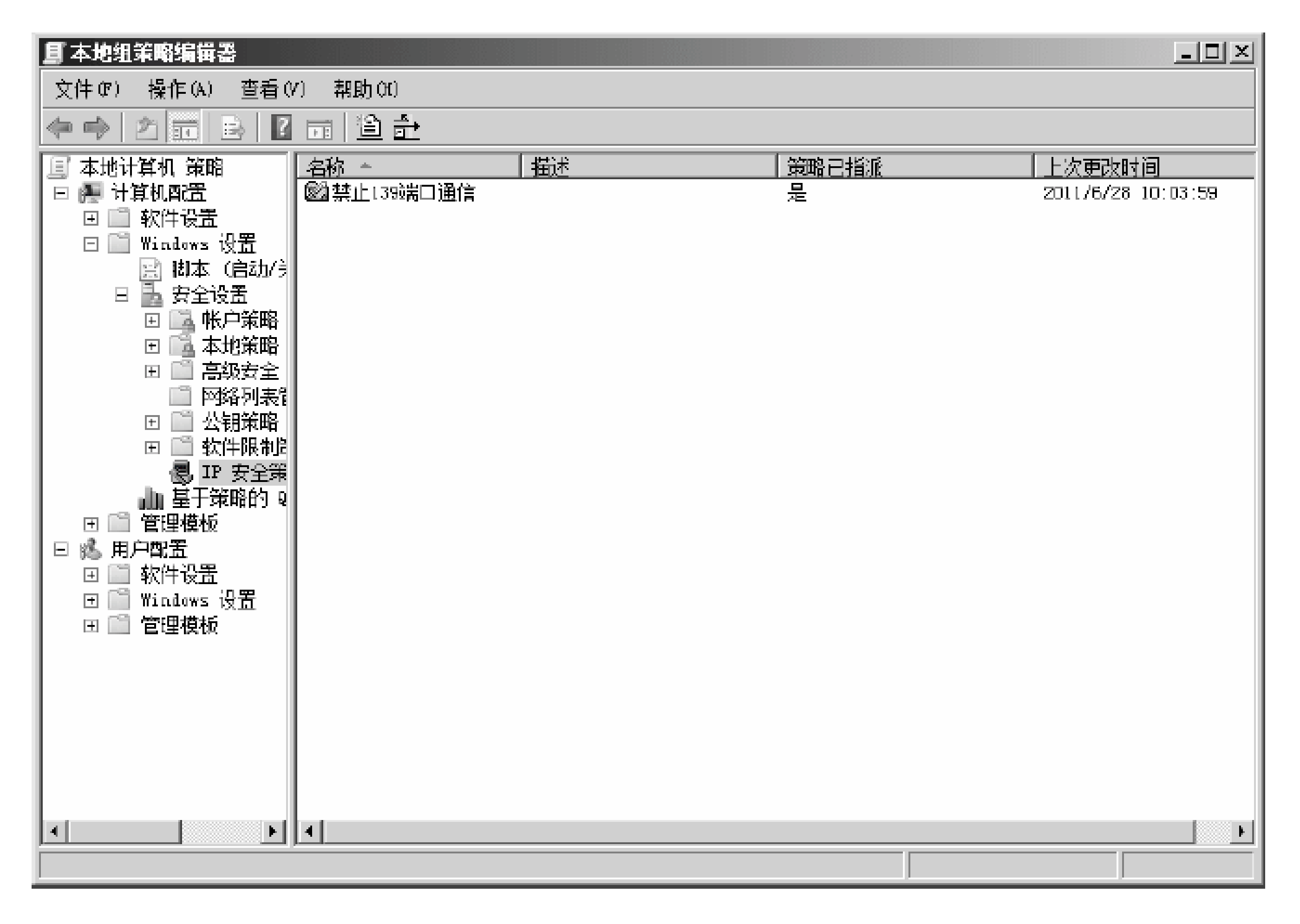


图 11-59

11.3　Windows 组策略安全

通过对组策略的管理，Windows Server 2008 可以对计算机的用户配置和计算机配置进行安全管理，加强计算机的安全性。当然对于服务器来说，组策略更多的针对安全策略和软件限制策略进行设置，以提高服务器的安全性。

11.3.1　安全策略

Windows Server 2008 的安全策略主要针对计算机的账户锁定、密码、用户权限和其他安全选项进行管理。

1. 账户策略

账户策略主要是对计算机的密码策略和账户锁定进行管理，作为系统管理员应该合理的设置账户策略，及时的更改密码信息，防止服务器被未授权的用户访问。

设置账户策略的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“gpedit.msc”命令，如图 11-60 所示，单击【确定】按钮。

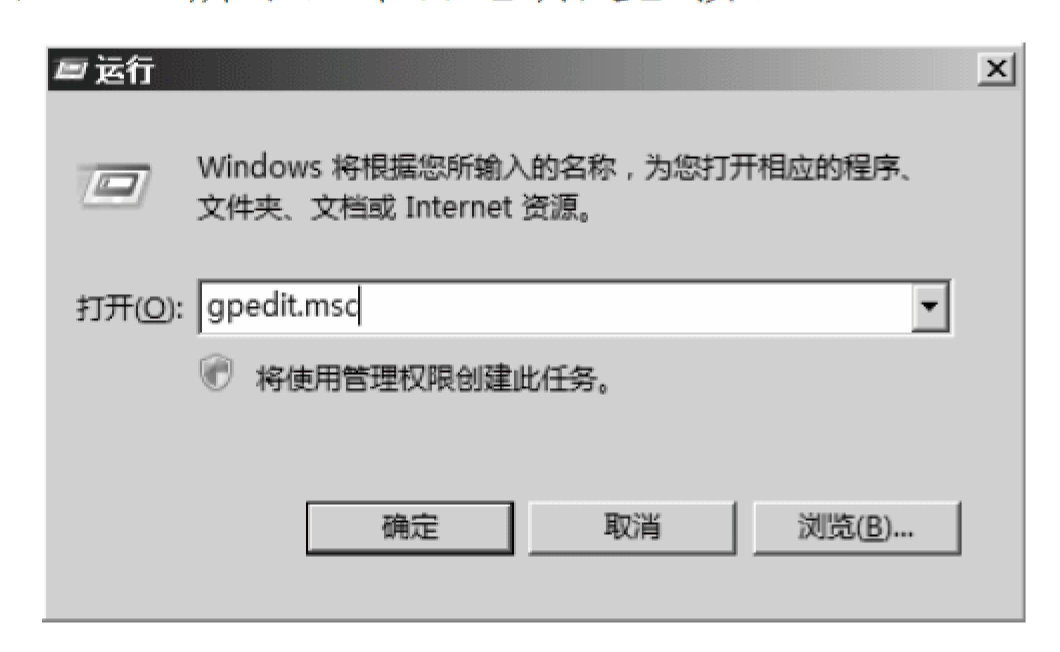


图 11-60

02 弹出【本地组策略编辑器】窗口，在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【账户策略】➢【密码策略】选项，在右边可以看到密码策略设定的相关内容，如图 11-61 所示。



图 11-61

密码策略设定的相关内容介绍如下。

- 密码必须符合复杂性要求：如果启用该功能，则计算机用户的密码必须包含大写字母、小写字母、数字、特殊字符中的三种，并且密码的长度至少 6 个字符。
- 密码最长使用期限：设置密码最长的使用期限，用户在登录时，如果密码的使用期限已到，则系统会要求用户强制更改密码；如果设为 0 则密码没有使用期限，默认值为 42。
- 密码最短使用期限：用来设置密码的最短使用期限，在该期限内用户不得更改密码。如果

设为 0，表示用户可以随时更改密码，默认值为 0.

- 强制密码历史：用户以前设置的密码不能被重复使用的个数，默认值为 0，表明可以被随意重复使用。
- 密码长度最小值：表明设置的密码最小应该为几个字符，默认值为 0，表明可以没有密码。
- 用可还原的加密来储存密码：系统密码是自动被加密的，当应用程序需要读取系统密码的时候密码需要被解密，如果需要应用程序读取系统密码，就应该选择该选项。

03 在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【账户策略】➢【账户选定策略】选项，在右边可以看到账户锁定策略设定的相关内容，如图 11-62 所示。



图 11-62

账户锁定策略设定的相关内容介绍如下。

- 账户锁定阈值：账户在进行登录的时候，登录失败多少次后账户就被自动锁定。默认值为 0，表明永远不会被锁定。
- 账户锁定时间：如果账户被锁定，在管理员没有手动解锁的情况下，多长时间后自动解锁。如果将锁定时间设为 0 表明账户在锁定后不会被自动解锁，除非由系统管理员手动解除锁定。
- 复位账户锁定计数器：用来记录用户登录失败的次数，当用户登录失败的次数超过登录账户锁定阈值，账户就会被锁定，一旦账户登录成功，锁定计算器的值就会被归零。

2. 本地策略

本地策略主要包含用户权限分配和计算机安全选项，通过对本地策略的设定，可以有效的控制用户的权限和计算机的安全。

配置本地策略的具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，弹出【运行】对话框，在【打开】文本框中输入“gpedit.msc”命令，如图 11-63 所示，单击【确定】按钮。



图 11-63

02 弹出【本地组策略编辑器】窗口，在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【本地策略】➢【用户权限分配】选项，在右边会看到用户权限分配的内容，如图 11-64 所示。

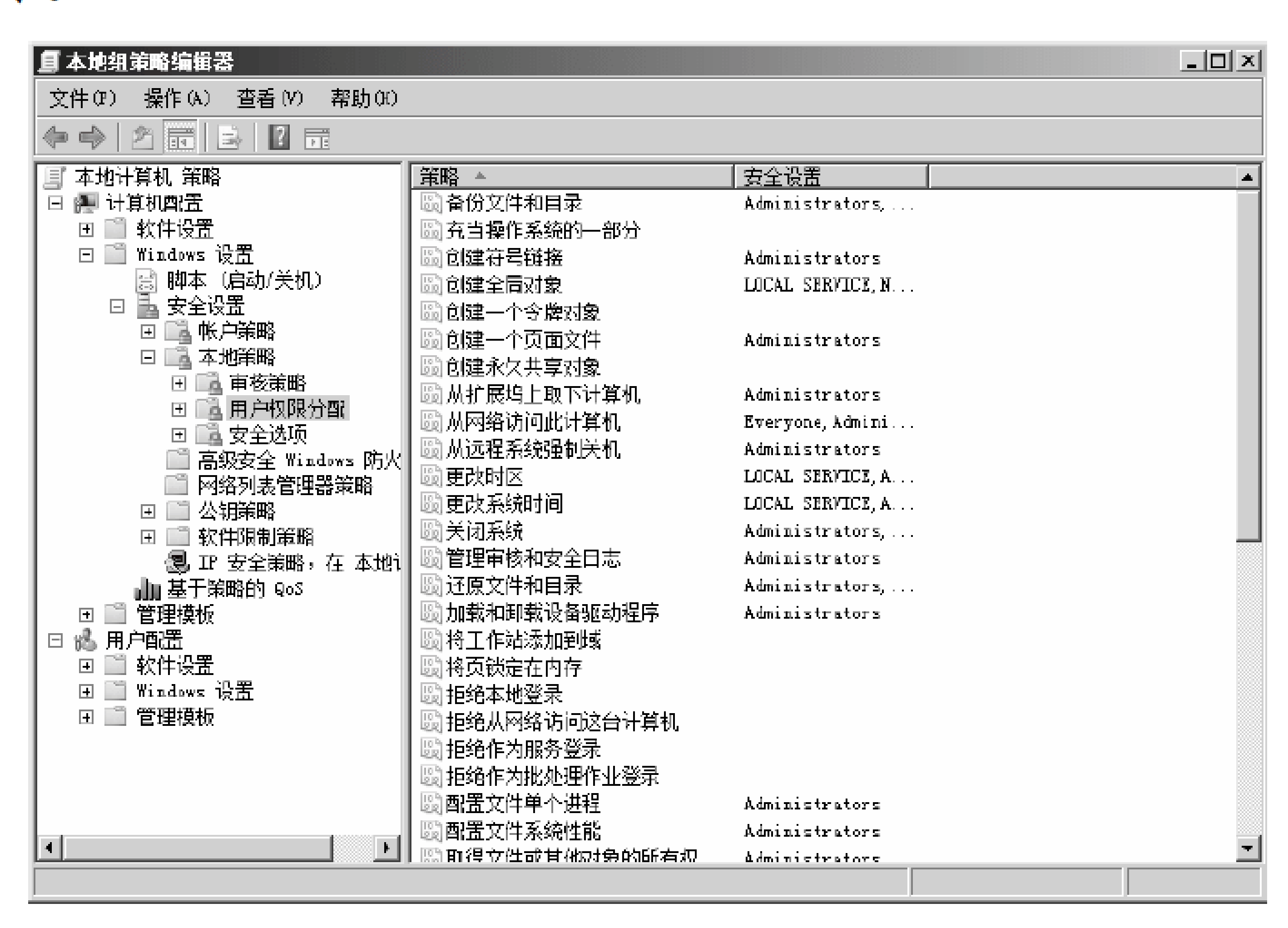


图 11-64

03 在用户权限分配策略中，如果要赋予某个用户某种权利，双击该项权利，将用户添加即可。比如要赋予某个用户有关闭系统的权利，则可以在【用户权限分配】策略中双击【关闭系统】选项，单击【添加用户和组】，将用户添加进去即可，如图 11-65 所示。



图 11-65

04 安全选项设定，单击【安全选项】策略，在右侧会看到安全选项策略的相关内容，如图 11-66 所示。

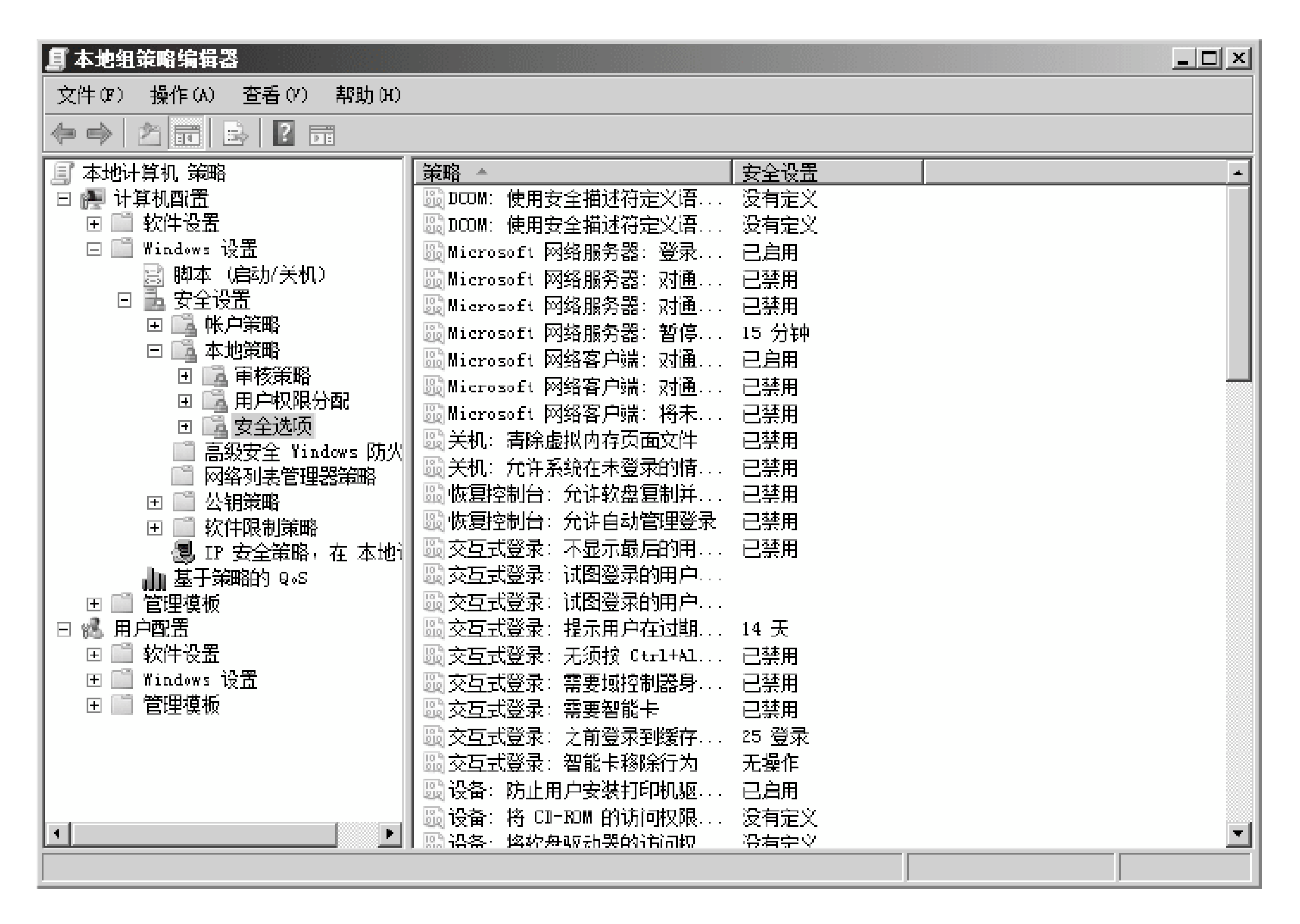


图 11-66

下面举几个常用的用户权限分配策略进行说明。

- 允许在本地登录：允许用户在本台计算机进行本地登录。
- 拒绝本地登录：拒绝用户在本台计算机上进行本地登录。
- 关闭系统：允许用户关闭计算机。
- 更改系统时间：允许用户更改计算机内部的系统日期、时间。
- 管理审核和安全日志：允许用户指定要审核的事件，也允许用户查询与清除安全日志。
- 装载和卸载设备驱动程序：允许用户加载与卸载外设驱动程序，也就是允许用户添加与删除硬件。

05 在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【本地策略】➢【安全选项】选项，安全选项主要是针对计算机进行安全设定的，如果要对某项策略进行更改，直接双击该策略，然后进行相应选择即可。比如用户在交互式登录时，不想让按 Ctrl+Alt+Del 组合键，则可以直接双击【安全选项】中的【交互登录：无须按 Ctrl+Alt+Del 属性】命令，然后选择【已禁用】单选按钮，如图 11-67 所示，单击【确定】按钮即可。



图 11-67

下面介绍常用的安全选项策略设定。

- 交互式登录——无须按 Ctrl+Alt+Del 键：计算机启动后不需要按 Ctrl+Alt+Delete 组合键，直接出现 Windows 登录界面。
- 交互式登录——不显示上次登录的用户名：计算机启动过后出现的 Windows 登录窗口中，是否显示上次登录的用户名。
- 关机——允许系统在未登录的情况下关闭：账户在未登录 Windows 之前是否允许关闭计算机。
- 账户——管理员账户状态：设定管理员账户的状态是禁用还是启用。
- 账户——来宾账户状态：设定来宾账户的状态是禁用还是启用。

11.3.2 软件限制策略

软件限制策略主要是帮助用户控制在服务器上应用程序的安装和应用程序的使用，使用组策略的软件限制策略，可以通过规则来标示并设置安全级别来指定软件是否运行从而保证服务器系统的安全性。在服务器上实行软件限制策略，本实例中要求服务器只能运行 IIS 服务。

具体操作步骤如下。

01 单击【开始】➢【运行】菜单命令，在弹出的【运行】对话框中输入“gpedit.msc”命令，如图 11-68 所示，单击【确定】按钮。

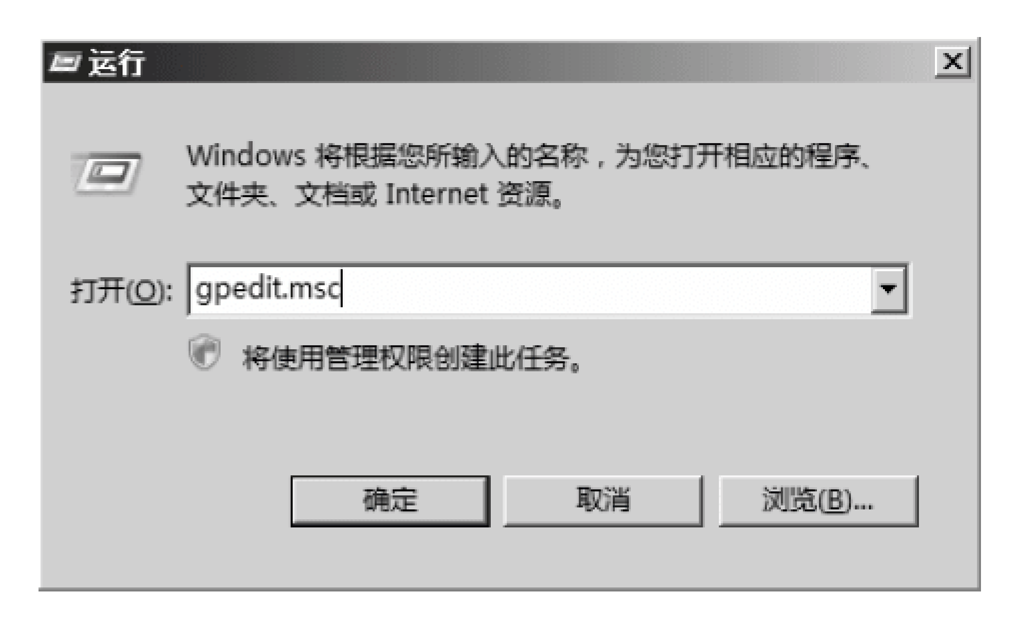


图 11-68

02 弹出【本地组策略编辑器】窗口，在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【软件限制策略】➢【安全级别】选项，在右侧选项列表中双击【不允许的】选项，如图 11-69 所示。

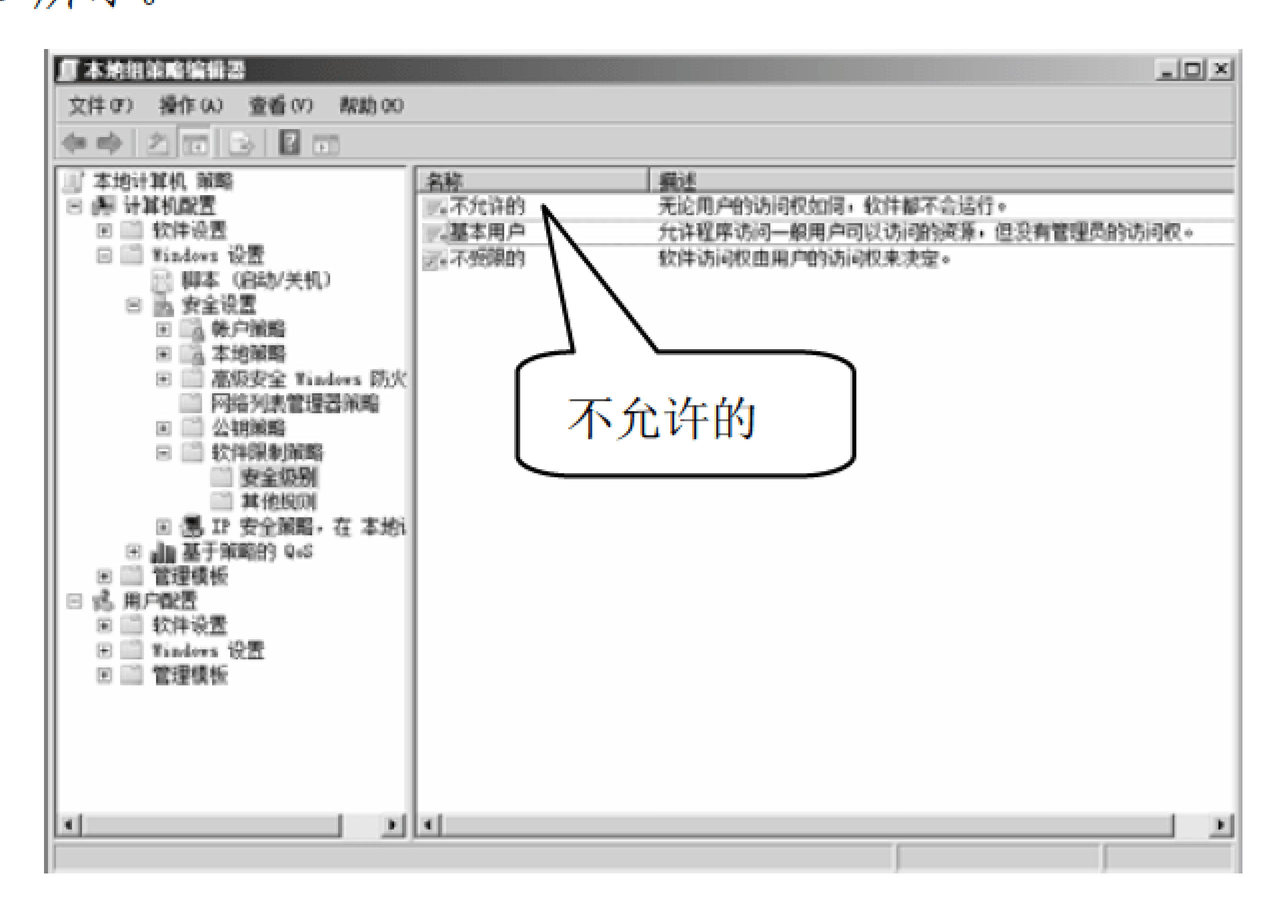


图 11-69

03 弹出【不允许的 属性】对话框，单击【设为默认】按钮，如图 11-70 所示。



图 11-70

04 弹出【软件限制策略】提示框，单击【是】按钮，如图 11-71 所示，则服务器将不能运行所有程序。

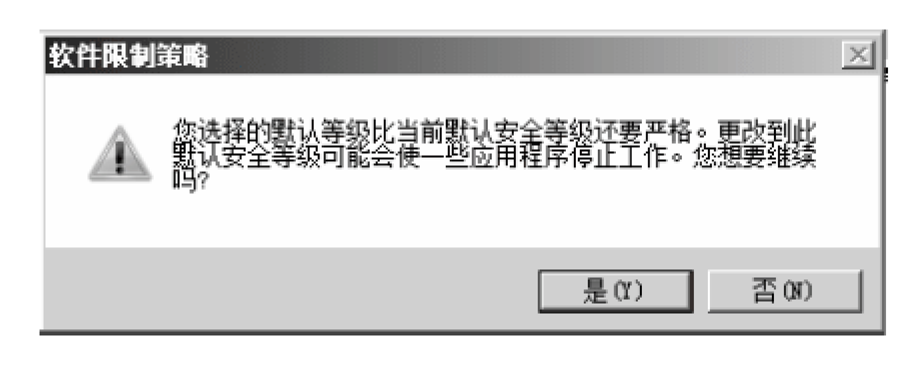


图 11-71

05 返回【不允许的 属性】对话框，如图 11-72 所示，单击【确定】按钮。

06 在左侧选项列表中选择【计算机配置】➢【Windows 设置】➢【安全设置】➢【软件限制策略】➢【其他规则】选项，在右边空白处右击鼠标，在弹出的快捷菜单中选择【新建路径规则】菜单命令，如图 11-73 所示。



图 11-72

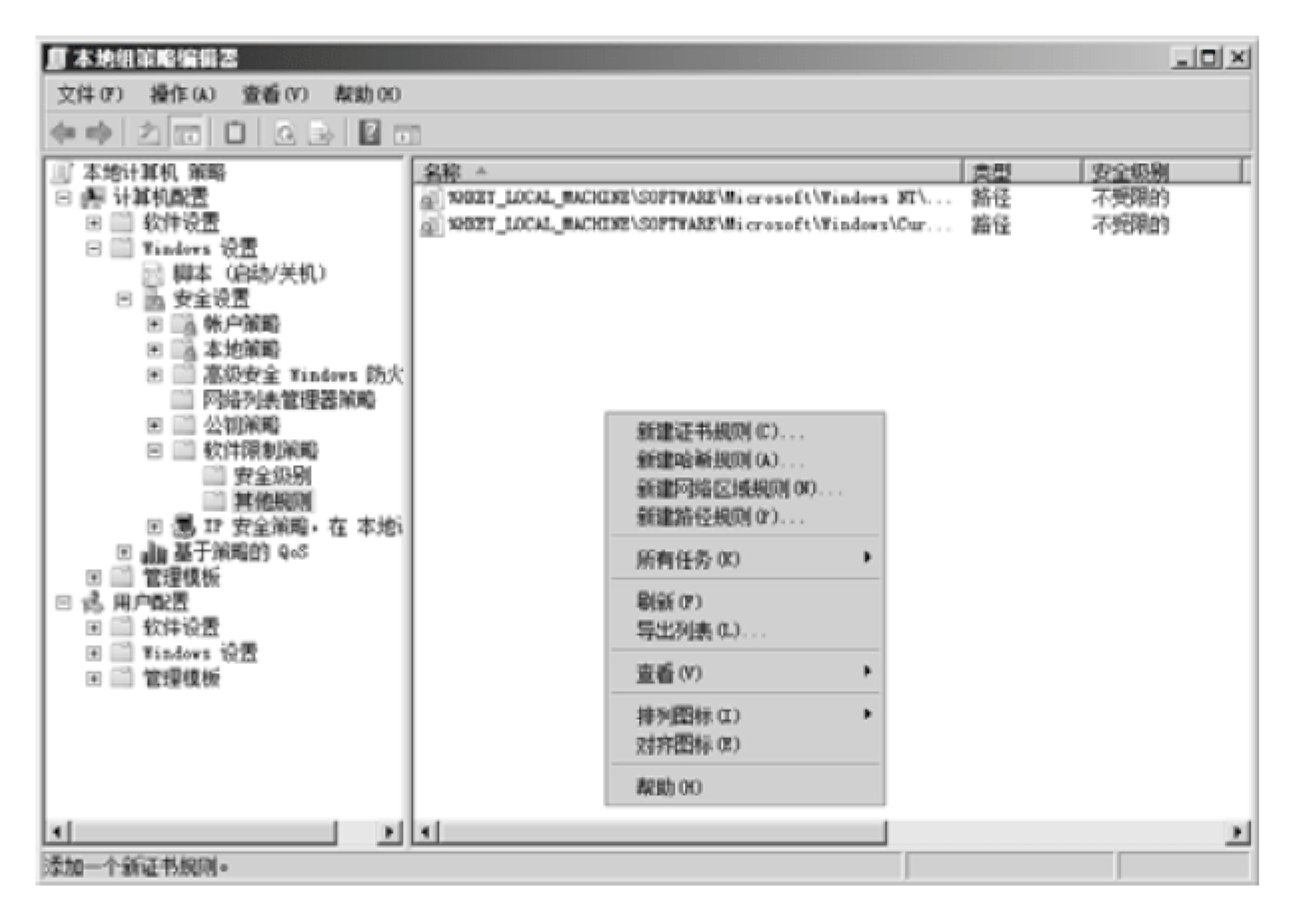


图 11-73

07 弹出【新建路径规则】对话框，单击【浏览】按钮，选择路径为“C:\Windows\system32\inetsrv”，需要注意的是，这里选择的路径是想要服务器运行的程序的安装目录，本实例中选择的路径为 IIS 的安装路径，在【安全级别】下拉列表中选择【不受限的】选项，如图 11-74 所示，表明可以不受限的访问 IIS 管理器，单击【确定】按钮。

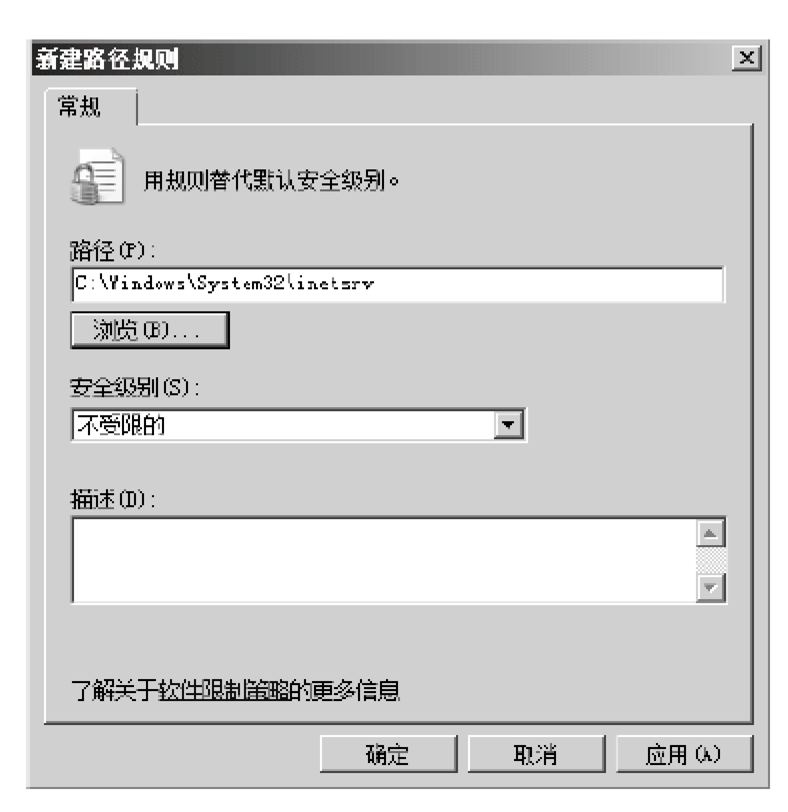


图 11-74

08 打开“C:\Windows\system32\inetsrv”目录，双击运行 InetMgr.exe 程序，如图 11-75 所示。

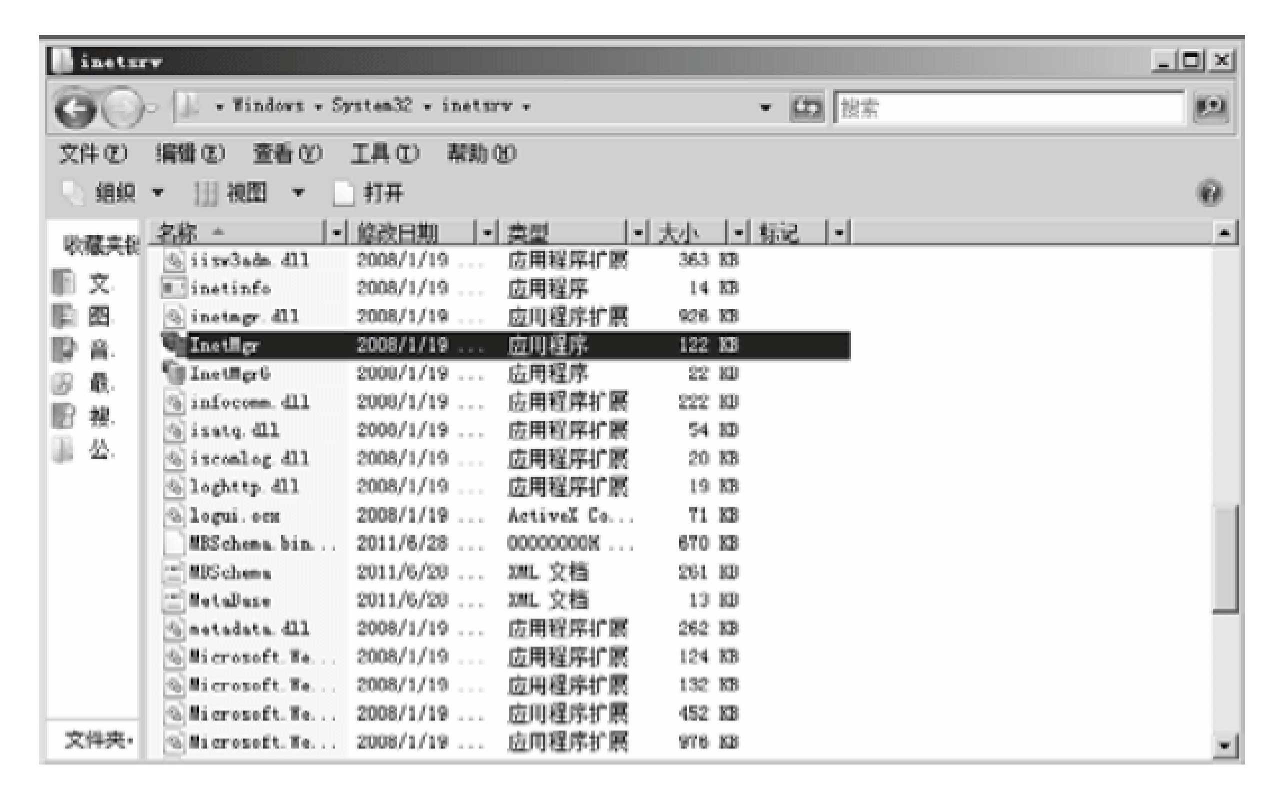


图 11-75

09 直接打开 IIS 管理器，如图 11-76 所示。



图 11-76

10 选择【开始】➢【所有程序】➢【管理工具】➢【Internet 信息服务器（IIS）管理器】菜单命令，弹出阻止提示，如图 11-77 所示。

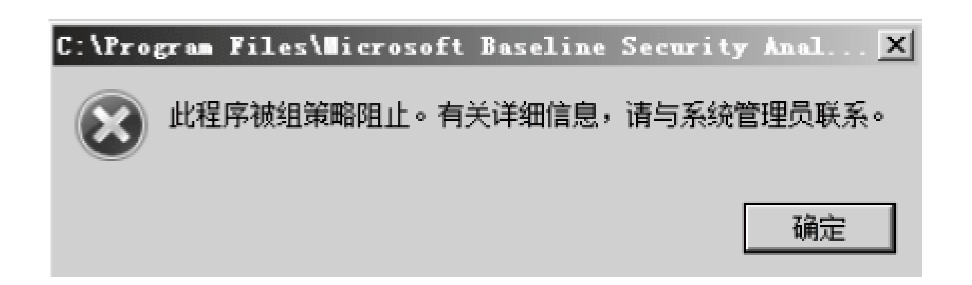


图 11-77



出现信息提示框的原因是，这种打开 IIS 管理器的方式是利用快捷方式连接至 IIS 安装目录打开的，但用户并没有将 IIS 管理器的快捷方式所在的目录放置在软件限制策略的路径规则中，因此在打开的时候会提示此程序被策略阻止。

11.4　项目实施：加强 Internet 信息服务安全

Internet 信息服务是 Windows 服务器系统用来发布网站的一个组件，是 Windows 服务器中最常用的一个服务，因此熟练的掌握如何加强 Internet 信息服务的安全性就成为了每个网络管理员必备的知识之一。加强 Internet 信息服务器安全的具体操作步骤如下。

01 进行漏洞扫描和系统升级。

02 关闭不需要的服务，只开启与 Internet 信息服务运行和系统运行必须的服务。

03 对组策略进行优化，针对 Internet 信息服务相关的用户设置权限以及服务器的安全设定。

04 开启 Windows 系统防火墙或者使用 IP 安全策略，禁止除了 Internet 信息服务之外的所有通信端口。

05 针对 Internet 信息服务的数据进行 NTFS 权限设置。

11.5　专家答疑

（1）新安装的 Windows Server 2008 有很多漏洞，是不是每一个漏洞都需要安装补丁？

答：并不是每个漏洞都需要安装补丁，漏洞补丁的安装需要根据系统的实际需求，以及漏洞的危害等级来进行安装。在重要的服务器上安装漏洞之前，最好做好数据备份和安装测试，以免造成数据丢失。

（2）系统端口是不是开启的越少越好？

答：是的。计算机与计算机之间的通信最终是要具体到端口号的，无论是正常访问某个计算机还是非法访问某个计算机都需要依靠端口来进行。因此计算机开启的端口越少，系统被非法方向的几率就越小。一般来说，服务器应该只开启必须运行的服务，其余的服务都关闭。

（3）针对服务器的实际需要，对组策略进行了设定，但是经过检查无误后，组策略的设定并没有即时的应用。

答：针对组策略的更改，默认值为 15 分钟生效，当然有些策略的更改是立即生效的。如果经过检查无误后，组策略的设定还是没有生效，可以将计算机重新启动下，组策略的更改就会随计算机的启动而生效。

第 12 章　网络设备安全配置

网络环境中包含的设备有路由器、交换机、服务器、终端客户机、防火墙、存储设备等。在实施网络安全加固时，大多数人都会把精力放在服务器、终端客户机、防火墙、存储等设备上，往往忽略了路由器、交换机等网络设备的配置，这是不对的。本章以 Cisco 网络设备为例，详细介绍网络设备的安全配置方法。

12.1　网络设备安全概述

作为网络环境中重要组成设备之一，网络设备的安全是不容忽视的。然而很多网络管理员会把全部的精力放在服务器、客户机、防火墙等设备的安全配置上，对网络设备的安全却不怎么关注，这一行为往往会造成巨大的网络安全隐患。为了更有针对性的进行网络设备安全配置，下面详细介绍网络设备可能存在的安全隐患，以及它可以提供的安全功能。

首先，傻瓜式交换机、路由器通常是被用在最底层的，这些设备不能进行管理配置，所以设备本身不存在安全问题，不在安全考虑范围之内。

其次，可通过 Console 控制口、Telnet、SSH、AUX 拨号连接等方式访问配置的设备，因配置信息可以控制网络通信，一般都具有网络安全问题。而这类设备一般都存在较大的安全隐患。

网络安全隐患主要表现在以下几个方面。

1. 人为的配置错误

人无完人，在网络设备的日常配置管理过程中，技术人员无论技术水平好坏，都有可能因为操作失误或配置错误，使设备存在安全隐患。这类隐患一旦产生，想要排查出来就很麻烦了。一般人为配置错误导致的安全隐患主要表现为以下几点。

（1）使用了空密码、较简单密码、默认密码，或者明文密码，而未设置加密保护。

（2）没有对远程网络管理设备配置访问控制策略，使得所有终端主机对网络设备都有配置权限。

（3）访问控制配置不合理或者配置错误，导致未能达到预期目的。

2. 网络设备的镜像系统存在漏洞

网络设备的操作系统用于控制设备运行、数据转发、路由计算、访问控制等，网络设备能否

正常运行，完全由它来决定。目前网络厂商比较繁杂，每个厂商的设备型号也比较多，但无论是哪一款设备，都存在有不同程度的系统漏洞，尤其一些小厂商的设备，漏洞更是五花八门。

一般因网络操作系统漏洞导致的安全威胁主要表现为以下几点。

（1）系统不稳定，负载能力弱，易出现系统瘫痪。

（2）数据包校验能力弱，易接收大量非法、畸形数据包，从而导致系统服务的拒绝访问和内容泄露。

（3）系统安全漏洞多，设备容易被完全控制。

3. 网络设备出厂时多余的默认服务

几乎所有设备在出厂时都会做一些默认配置，比如 HTTP、NTP、CDP 等特定的网络服务都会被开启，而这些服务都有可能被攻击者利用，成为攻击网络的跳板。利用这些不安全的服务，攻击者可以对设备进行远程拒绝服务攻击，或者借此获取设备基本信息、完全控制网络设备。

4. 网络设备固件存放不当，被攻击者物理接触

网络设备一旦被攻击者物理接触，就有可能被攻击破坏。这主要是通过非法连接串口、非法恢复默认密码、非法关机等方法实施攻击。具有这类安全隐患的设备一般都是处于公共场所，且加锁保护措施不完善。

12.2 网络设备安全配置

路由器、交换机等网络设备涉及的网络安全保障技术比较多。从现实应用角度出发，做如下详细介绍。

12.2.1 硬件安全

网络设备的主要作用是保证网络环境通畅，并按照指定策略传输信息，是信息业务应用中重要的通信节点，一旦该类设备物理损坏，会造成极大的损失。

通常网络设备的硬件安全要从以下几个方面考虑。

首先，网络设备安装配置时需要保证设备的安全、稳定运行，这就需要确保工作环境具备适宜的温度和湿度，良好的通风效果，同时还要具备防火、防盗、防静电、防电磁干扰等条件。一般网络设备都会放置在专业的服务器、设备机房中，如图 12-1 所示。机房内有可调控温度的设备，而且要保证无尘操作，应尽量少进入机房操作设备，大型的机房在进入时还需要穿戴防尘衣。



图 12-1

其次，并不是所有设备都存放在机房，很多网络设备会安放在建筑的不同位置。比如在网吧、小区的墙壁上经常会看到存放设备的机柜，在街道上也有很多的运营商设备。这些存放于公共场所的设备自带的 Console（控制）口，如果管理不善，很容易被不法分子利用，以此进入设备、控制网络。所以这类设备一般要保证有加锁机柜，安放高度合适，有条件的还要在重要设备附近安置监控设备，如图 12-2 所示。



图 12-2

12.2.2 口令安全

网络设备的配置接入方法有很多种，Console 口配置、AUX 口拨号连接、Telnet 远程控制、HTML 网页配置。无论是哪一种方法，都有很大的权限修改设备的配置信息，如果随意的被连接会对网络正常使用造成很大的威胁，所以这些配置接入方法一般都需要配置访问口令。下面针对网络设备的

口令安全作详细的介绍。

1. 默认口令隐患多

大部分的网络设备在出厂时都有默认用户名和口令，比较常见的有“admin”、“guest”。利用这些默认的口令，只要攻击者接入网络，就可以登录该网络的设备进行操作。

而在现实环境中，很多网络管理员出于方便记忆和对网络安全性过于信赖等因素，一直使用默认用户名和密码，这和不做密码保护几乎没什么区别。

2. 安全口令的配置管理规范

网络设备提供了多机口令，包括：常规模式口令、特权模式口令、配置模式口令、Console 控制口连接口令、Telnet 连接口令、SSH 连接口令等。在复杂的网络环境中，每一个口令都是一个安全屏障，所以在配置设备时尽量要配置所有的口令，同时各个口令的密码要有区分，以确保每一个口令都是有意义的。除此之外，不同的设备口令配置也不能相同。

在进行口令配置时，口令应具备以下特征。

（1）口令应具备复杂性，最好由数字、字母、符号三种字符组成。

（2）口令长度不宜过短，6~8 位以上安全性较高，不易破解。

（3）口令不建议使用生日、人名、公司信息等具有特殊意义的字符串。

日常管理中，可以制作一套口令表，方便查看和记忆。但在使用时，口令可能随时被泄露，所以需要管理员定期更新一些口令，并且在获悉口令泄露后及时的更改口令。

3. 特权模式的口令配置

使用任何一种设备配置接入方式，都需要从用户模式进入到特权模式。如果只设置了 Telnet 远程登录密码，没有配置特权模式密码，就只能进入到用户模式，所以想要通过远程连接正常配置设备，必须要配置特权模式密码。下面以 Cisco 路由器为例详细介绍一下特权模式口令的配置方法。

```
Router>enable
//进入特权模式
Router#configure terminal
//进入全局配置模式
Router(config)#enable password cisco
//配置特权模式明文口令“cisco”
Router(config)#enable secret cisco
//配置特权模式密文口令“cisco”
Router#show running-config
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
//查看配置信息，“secret”后的“5”表示使用的是 MD5 加密认证
```

4. Telnet 远程登录口令配置

远程 Telnet 登录设备时，使用的是设备的 VTY 口。网络设备默认有五个端口供远程终端客户机连接，也就是 0~4 五个虚拟接口，在进行配置时要同时对五个虚拟接口配置登录口令。具体操作步骤如下。

```
Router(config)#line vty 0 4
//进入虚拟接口 0~4 的配置子模式
Router(config-line)#login
% Login disabled on line 66, until 'password' is set
% Login disabled on line 67, until 'password' is set
% Login disabled on line 68, until 'p
assword' is set
% Login disabled on line 69, until 'password' is set
% Login disabled on line 70, until 'password' is set
//开启登录功能，开启后提示允许给五个虚拟接口配置密码
Router(config-line)#password cisco
//配置 VTY 口令"cisco"
Router#show running-config
line vty 0 4
 password cisco
 login
//查看配置信息
```

5. Console 控制口安全配置

使用配置线直接连接设备配置时，使用的是串口及 Console 控制口。下面详细介绍 Console 控制口口令的配置步骤。

```
Router(config)#line console 0
//进入 Console 口的配置子模式
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
//开启登录功能，开启后提示允许给 Console 控制口配置密码
Router(config-line)#password cisco
//配置 Console 控制口口令"cisco"
Router#show running-config
line con 0
 password cisco
 login
//查看配置信息
```

6. 为所有口令加密

大部分口令默认明文显示，这样很不安全，所以在配置完所有口令后，需要对设备口令进行统一加密，操作命令如下。

```
Router(config)#service password-encryption
加密后，查看配置信息。
Router#show running-config
service password-encryption
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password 7 0822455D0A16
!
line con 0
 password 7 0822455D0A16
```

```
 login
line vty 0 4
 password 7 0822455D0A16
 login
```

12.2.3　基于 MAC+IP+VLAN+端口的绑定

在网络环境中经常会出现地址冲突、地址欺骗的现象。某些终端客户机因手工配置或感染木马等原因，使自己的地址信息和服务器或其他主机地址信息发生冲突，进而影响到整个网络的正常使用，比如常见的 ARP 地址欺骗。

普通主机之间发生冲突，可能影响不是很大，主机提示冲突后重新配置新地址就可以了。但是有些服务器或网络设备在网络中的位置至关重要，一旦出现地址冲突，会对网络业务服务造成巨大的影响，如 WEB 服务器、设备管理地址、网关等。

下面主要介绍几种常用的地址绑定方法。

1. 基于端口的 MAC 地址绑定

可以规定某一接口允许通过的 MAC 地址来实现绑定。下面以 Cisco 2950 交换机为例进行配置。

```
Switch>enable
//进入特权模式
Switch#configure terminal
//进入全局配置模式
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 端口的配置子模式
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port
//配置开启端口安全模式
Switch(config-if)#switchport port-security mac-address 0001.AB3D.32EA
//将某主机的 MAC 地址"0001.AB3D.32EA"绑定到该端口，允许主机通过该端口访问网络
Switch(config-if)#no switchport port-security mac-address 0001.AB3D.32EA
//删除绑定主机的 MAC 地址"0001.AB3D.32EA"。
Switch(config-if)#switchport port-security maximum 30
//最大允许验证通过的 MAC 地址数，本实例设为"30"
```

2. 基于扩展访问控制列表的 MAC 地址绑定

平时接触的访问控制列表大都是基于 IP 地址和端口的，事实上，基于 MAC 地址也是可以实现访问控制功能，进而实现 MAC 地址绑定的。下面以 Cisco 3560 交换机为例进行配置。

（1）创建访问控制列表

```
Switch(config)#Mac access-list extended MAC
//创建一个 MAC 地址访问控制列表，并命名为 MAC
Switch(config-ext-macl)#permit host 0001.AB3D.32EA any
//定义 MAC 地址为"0001.AB3D.32EA"的主机可以访问任意主机
Switch(config-ext-macl)#permit any host 0001.AB3D.32EA
//定义所有主机可以访问 MAC 地址为"0001.AB3D.32EA"的主机
```



默认在访问控制列表最后有一条“deny any any”隐藏命令，以拒绝其他所有 MAC 地址的访问请求。

（2）应用访问控制列表

```
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 端口配置子模式
Switch(config-if)#mac access-group MAC in
//在 fastEthernet 0/1 端口应用访问控制列表“MAC”。
```

（3）删除访问控制列表

```
Switch(config)#no mac access-list extended MAC
```

3. 基于 IP 地址和 MAC 地址的绑定

在很多网络环境下，IP 地址是不可以随意更改使用的，变更 IP 地址很容易造成地址被盗用或冲突。比如某一 IP 地址在网络中具有访问其他资源的特权，一旦被不法分子在其他主机盗用就麻烦了。

如果只使用前两种方式，就只能限制允许通过的 MAC 地址，但是达不到 MAC 和 IP 地址绑定的功能。必须想办法让 IP 地址和 MAC 地址一一对应起来。下面介绍详细配置方法。

使用 ARP 命令绑定 IP 和 MAC 对应关系，将 IP 地址“192.168.100.100”和 MAC 地址“0001.AB3D.32EA”绑定在一起。

```
Router(config)#arp 192.168.100.100 0001.AB3D.32EA ARPA
```

4. 基于 IP 地址和交换机端口的绑定

可以将 IP 地址与交换机端口也绑定在一起，这样一来该端口就只能由对应的 IP 地址使用，使用其他 IP 地址连接会立刻断网，有效的防止了乱改 IP 的行为。下面介绍详细配置方法。

```
Router(config)#access-list 1 permit 192.168.100.100
//定义一条允许 IP 地址“192.168.100.100”通过的访问控制列表，编号为 1。
Router(config)#interface fastethernet0/1
//进入需要实施绑定的端口“fastethernet0/1”的配置子模式。
Router(config-if)#ip access-group 1 in
//在端口配置子模式下应用访问控制列表 1。
配置后在 fastethernet0/1 端口只允许 IP 地址 192.168.100.100 的主机连接网络。
```

12.2.4　过滤安全端口

在网络中有很多具有安全隐患，可以被攻击者用于实现网络攻击的端口，比如 113、135、137、138、139、445、593、1023、1029、1434、2745、3127、6129、5554、4168 等。这些端口种类繁多，有系统服务端口、软件漏洞端口、病毒木马后门端口，无论哪一个端口被利用，都有可能造成网络设备或服务器被完全控制，所以在实现网络安全配置时，一定要想办法将这些端口屏蔽掉。

虽然大多数服务器都有防护网络攻击、过滤安全端口的配置，但为了更好的保证整个网络环境的安全，这些不安全端口访问到网络设备时就应该被过滤掉。这主要依靠 ACL 访问控制来实现，下面介绍详细配置方法。

（1）创建扩展访问控制列表 100

```
Router(config)#access-list 100 deny tcp any eq 113 any
Router(config)#access-list 100 deny tcp any eq 135 any
Router(config)#access-list 100 deny udp any eq 135 any
Router(config)#access-list 100 deny tcp any eq 137 any
Router(config)#access-list 100 deny udp any eq 137 any
Router(config)#access-list 100 deny tcp any eq 138 any
Router(config)#access-list 100 deny udp any eq 138 any
Router(config)#access-list 100 deny tcp any eq 139 any
Router(config)#access-list 100 deny udp any eq 139 any
Router(config)#access-list 100 deny tcp any eq 161 any
Router(config)#access-list 100 deny udp any eq 161 any
Router(config)#access-list 100 deny tcp any eq 445 any
Router(config)#access-list 100 deny udp any eq 445 any
Router(config)#access-list 100 deny tcp any eq 593 any
Router(config)#access-list 100 deny tcp any eq 1024 any
Router(config)#access-list 100 deny tcp any eq 2745 any
Router(config)#access-list 100 deny tcp any eq 3127 any
Router(config)#access-list 100 deny tcp any eq 3389 any
Router(config)#access-list 100 deny udp any eq 3389 any
Router(config)#access-list 100 deny tcp any eq 6129 any
```



由于安全端口比较多，本实例不再一一配置。在配置时还应注意，在过滤端口时要明确指定其属于 TCP 端口还是 UDP 端口，像 113 端口就是 TCP 端口，而 135 端口既有 TCP 端口又有 UDP 端口。虽然同是 135 端口，但是 TCP 和 UDP 完全不同，要分别写出。

（2）在设备入口方向应用访问控制列表

```
Router(config)#interface fastethernet0/1
Router(config-if)#ip access-group 1 in
```



在流量进入设备之前就应该过滤掉，这样可以避免设备处理这部分流量的消耗。

12.2.5 正确配置认证协议

网络设备连接时，会用到很多协议，为了保证安全，有不少协议都允许实施认证，比如广域网协议 PPP 的 PAP 和 CHAP 认证，路由协议 OSPF 的认证。在网络环境比较复杂的情况下，尽量要配置所有可实施认证的协议，并且选择认证强度比较高的技术，比如选择 CHAP 认证而不选 PAP，又或者使用 OSPF 协议的加密认证而不实用明文。下面以 OSPF 路由协议的加密认证为例进行介绍。

假设路由器 R1 和 R2 直连，并运用 OSPF 路由协议相互学习路由信息。为了保证路由信息不被其他外来设备学习到，在 R1 和 R2 之间做区域的 MD5 认证。配置命令如下。

```
R1(config)#interface s1
//进入 interface s1 端口配置子模式
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
//使用 MD5 身份验证，定义认证密钥，密钥字符串为“cisco”
R1(config)#router ospf 100
//配置 OSPF 协议，进程号为 100
R1(config-router)#area 0 authentication message-digest
//指定身份验证
R2(config)#interface s1
//进入 interface s1 端口配置子模式
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
//使用 MD5 身份验证，定义认证密钥，密钥字符串为“cisco”
R2(config)#router ospf 100
//配置 OSPF 协议，进程号为 100
R2(config-router)#area 0 authentication message-digest
//指定身份验证
```

12.2.6　使用安全的 SNMP 网管方案

SNMP（简单网络管理协议）是实施网络管理不可或缺的技术。使用 SNMP 协议，网络管理工作站可以轻松的获取各种网络设备的详细信息。但是 SNMP 协议的实现机制存在多个漏洞，这些漏洞可以允许非法越权访问、拒绝服务攻击、导致不稳定的运行状况，严重危害互联网基础安全。

目前 SNMP 的版本主要是 SNMPv1、SNMPv2 和 SNMPv3。虽然从安全鉴别机制来分析，SNMPv1 和 v2 两个版本较弱，而 SNMPv3 由于采用了新的 SNMP 扩展框架，安全性和管理上有很大的提高。但因为 SNMPv3 出现较晚，很多正在使用的旧设备不支持该版本，且大多数厂商普遍支持的还是 SNMPv1 和 v2 两个版本。这就导致了网络中依然大量存在 SNMP 安全隐患。从现实情况来看，管理员能做的只是让 SNMPv1 和 v2 版本的使用更安全一些。

导致安全威胁最明显的是“community string”。在许多网络设备和操作系统的 SNMP 协议实现中往往存在能进行 SNMP 写操作的默认“community string”，比如“public”。远程攻击者利用这些可进行写操作的“community string”能够获取服务器完全控制权限、修改路由器配置、重启或关闭设备。

解决 SNMP 的具体操作方法，详细介绍如下。

1. 过滤边界 SNMP 访问

攻击者通常处于外部网络，通过向边界设备发送 SNMP 请求信息，以查找漏洞实现攻击。而 SNMP 协议只要在内部网络正常运行即可满足管理的需要。所以，可以在边界设备外侧端口过滤所有的 SNMP 信息，以避免信息外泄和网络攻击。

SNMP 主要使用 161 和 162 两个 UDP 端口，需要配置 ACL 访问控制列表对应这两个端口的流量，具体配置命令如下。

01 创建访问控制列表 100，拒绝所有主机的 161 和 162 端口信息。

```
Router(config)#access-list 100 deny udp any eq 161 any
Router(config)#access-list 100 deny udp any eq 162 any
```

02 假设 fastEthernet 0/1 口为边界设备外网接口，应用访问控制列表 100。

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#ip access-group 100 in
```

2. 修改默认的“community string”

很多支持 SNMP 服务的产品的出厂设置中，默认的 community-string 值是“public”(只读访问)和“private”（读/写访问）。攻击者往往会使用这两个 community-string 扫描网络，实现网络攻击。所以在配置设备时，这两个默认口令一定要改掉。修改 community-string 的配置命令如下。

```
Router(config)#snmp-server community cisco rw
//将 community-string 值改为“cisco”，权限为“读写”
```

3. 过滤网络中不正常的 SNMP 访问

在网络系统中实施网络管理时，只有个别的网络管理系统需要发生 SNMP 请求。所以，网络管理系统中的 SNMP 代理（被管客户机）可以设置仅接受管理服务器发送的 SNMP 请求。这样可以降低内部攻击风险。

假设主机 192.168.100.100 为网络管理服务器，以 Cisco 路由器为例，在所有网络设备上需要做如下配置。

```
Router(config)#ip access-list standard snmp-server
//创建命名的访问控制列表“snmp-server”
Router(config-std-nacl)#permit 192.168.100.100
//编辑访问控制列表，允许 192.168.100.100 主机访问
Router(config-std-nacl)#exit
//返回全局配置模式
Router(config)#snmp-server community public rw snmp-server
//配置 SNMP 协议，community string 为“public”，权限为“读写”，该 SNMP 协议配置对访问控制列表“snmp-server”
生效
在配置网络设备的 SNMP Trap 配置时，也可以指定 Trap 信息的接收者，配置命令如下。
Router(config)#snmp-server host 192.168.100.100 traps trap
//SNMP Trap 的接收者为“192.168.100.100”，认证字符串为“trap”
```


提 示

如果网络管理允许，可以将设备的 SNMP 协议关闭。

12.2.7 防止 SYN 攻击

首先来认识一下什么是 SYN 攻击，这种攻击主要是利用 TCP 的三次握手机制来实现的，攻击端伪造大量的 IP 地址向被攻击端发出 SYN 包，建立 TCP 同步连接。出于三次握手机制的正常反应，被攻击端会返回大量的 SYN+ACK 包，这些返回的确认包根本就不可能发送到正确的目的地，在被攻击端等待连接超时关闭的过程中已经消耗了资源。这些消耗掉的资源超过一定的比例，就会严重影响到正常服务的应用。至此已经形成了 SYN 攻击，达到了攻击目的。

由此看来，只要能够拦截异常的 TCP 连接就可以防止 SYN 攻击了。为此大多数的路由器都植

入了 TCP 拦截（TCP intercept）功能，用于防止 SYN 泛洪攻击。在 TCP 连接请求到达目标主机之前，TCP 拦截通过对其进行拦截和验证来阻止这种攻击。

下面以 Cisco 路由器为例，详细介绍 TCP 拦截功能的配置。

1. 设置 TCP 拦截的工作模式

TCP 拦截主要有两种工作模式：拦截和监视。

拦截模式（intercept mode）：在拦截模式下，路由器会拦截所有的 TCP 同步请求，并分别以服务器和客户机身份，与原来的客户机、服务器机建立连接。如果两个连接都成功地实现，证明 TCP 同步连接请求是合法的，路由器会将两个连接进行透明的合并。在此过程中，路由器利用更为严格的超时限制，以防止其自身的资源被 SYN 攻击耗尽。

监视模式（watch mode）：在监视模式下，路由器会统计已返回 SYN+ACK 包，等待客户端确认超时的连接数量。如果在规定的时间内超过了指定的连接数，路由器可以执行关闭连接，同时还可以使用 ACL 访问控制列表定义要进行 TCP 拦截的源和目的地址。

虽然两种模式都可以实现防止 SYN 攻击，但是使用拦截模式会让路由器处理大量的请求包，加重了设备负担，会影响到整个网络的性能。所以通常建议选择监视模式。TCP 拦截监视模式开启的配置命令如下。

设置路由器工作模式，默认为“intercept”拦截模式，本实例选择“watch”监视模式。

```
Router(config)#ip tcp intercept mode (intercept/watch)
```

2. 监视模式参数配置

使用监视模式，如何判断设备是否遭受攻击呢？这主要依靠一些特定阈值来判断。这些阈值主要是 half-open 连接在执行不同操作的连接数，在介绍这些阈值之前，先来了解一下监视模式的工作方式。

（1）当路由器检测到的 half-open 连接数超过阈值，确认正遭受攻击时，路由器开始删除之前的连接，默认是最早的 half-open 连接（可以使用“ip tcp intercept drop-mode random”命令，随机关闭半开连接）。

（2）初始的重传超时时间被减少一半，直到 0.5 秒。如果处于监视模式，则超时时间减半，直到 15 秒。

在监视模式下，有两个值用于判断是否遭受攻击，并开始删除 half-open 连接。

```
Router(config)#ip tcp intercept max-incomplete high number 1100
//设置路由器开始删除连接之前，能够存在的 half-open 连接的最大数
Router(config)#ip tcp intercept one-minute high number 1100
//设置路由器开始删除连接之前，每分钟内能存在的最大 half-open 连接数
当 half-open 连接数降低至一定程度时，路由器认为攻击已经减弱或者不存在，停止删除 half-open 连接。
Router(config)#ip tcp inercept max-incomplete low number 900
//设置路由器停止删除 half-open 连接之前，能够存在的最大 half-open 连接数
Router(config)#ip tcp intercept one-minute low number 900
//设置路由器停止删除连接之前，每分钟内能存在的最小 half-open 连接数
```



half-open 连接总数与每分钟 half-open 连接的数量只要有任何一项达到最大值，TCP 拦截就会被激活，并开始删除 half-open 连接。在 TCP 拦截过程中，只有两个值都降低到指定的最低值，才会停止删除 half-open 连接。

3. 设置访问控制列表，指定需要保护的主机

执行 TCP 拦截时，可以监控指向特定服务器的请求，这就需要配置一条访问控制列表来指定这些服务器。配置命令如下。

```
Router(config)#access-list 101 permit tcp any host 192.168.100.100
//"192.168.100.100"为受保护的目标服务器
```

4. 开启 TCP 拦截

前面已经配置了监控模式及其参数，下面配置启用 TCP 拦截。配置命令如下。

```
Router(config)#ip tcp intercept list 101
//"101"是前面配置的指定受保护服务器的 ACL 访问控制列表
```

12.2.8 关闭 CDP 服务

思科发现协议（CDP）是工作在数据链路层上的协议，主要用来获取相邻设备的地址配置及平台信息。CDP 协议与设备介质无关，默认运行在所有的思科产品上。在故障排错、性能优化等方面有着不可替代的作用。但是，CDP 协议本身存在有巨大的安全问题。

CDP 协议在工作时，会向所有支持 CDP 协议的接口上周期性的发送设备基本信息，邻接设备间可以彼此学习所发送的信息，同时管理员也可以通过接收分析这些信息，实施网络排错和性能优化。但是这些信息同样可以被攻击者使用嗅探工具获取并利用。如果网络连接的是单一网络，所有设备都连接在同一个局域网中还比较安全，相反，如果网络连接到多个组织机构时，这个安全隐患就比较突出了。

CDP 协议毕竟有存在的优势，不应单一的为了安全就将其彻底关掉。作为网络管理员，应当做到安全和功能并重，既能够享受 CDP 协议所带来的优势，而又不被其安全问题所困扰。一般攻击者都处于外部网络，只要限制 CDP 协议信息从边缘设备发送出去，就可以避免其带来的大部分威胁，而内部网络攻击源很少，可以较放心的使用 CDP 协议。从分析中可以得出如下配置。

在所有边缘路由器连接外网的接口上禁用 CDP 服务。

```
Router(config)#interface s0/1
//进入边界路由器外网接口 s0/1 的配置子模式
Router(config-if)#no cdp enable
//关闭该端口的 CDP 服务
```



为了安全起见，也可以在全局配置模式下关闭 CDP 服务。

```
Router(config)#no cdp enable
```

在内部网络设备上，可以根据需求开启 CDP 服务。但是需要考虑开启的方式，是全局开启，还是指定端口开启。不必要的 CDP 流量越少越安全，所以建议针对端口，开启足够进行故障排错和性能优化使用的 CDP 服务即可。

12.2.9 关闭其他具有安全隐患的服务

在路由器、交换机生产出厂的时候，往往有一些不常用或者有可能产生安全隐患的服务被默认配置。为了保证设备安全，需要将这些服务关闭。下面详细介绍各种需要关闭的服务。

1. 关闭 BOOTP 服务器

BOOTP（自举协议）是一个基于 UDP 协议的协议。该协议主要应用于有无盘工作站的局域网中，它可以让无盘站从中心服务器上获得 IP 地址。和 DHCP 协议功能有些相似，BOOTP 为局域网中的无盘工作站分配动态 IP 地址。在网络设备上，使用 BOOTP 协议还可以实现设备 IOS 镜像的拷贝。

如果网络设备的 BOOTP 服务开启，很有可能使攻击者利用 BOOTP 服务下载到设备的配置文件，所以使用设备时，需要首先检查 BOOTP 服务有否开启，如果开启要马上关闭。关闭 BOOTP 服务的命令配置如下。

```
Router(config)#no ip bootp server *
//“*”代表匹配所有地址
```

2. 关闭 DNS 服务

默认情况下，Cisco 路由器 DNS 服务是被开启的。路由器会以 255.255.255.255 为广播地址发送查询信息。使用这个全网广播地址，任何主机都可以接受到查询信息。作为攻击者可能会借机伪装成一个 DNS 服务器，在真正的 DNS 服务器做出反应前，发送一个伪造的回复。通常情况下，路由器接收到多个回复时，只会应用第一个回复，后面的都会被丢弃。

本身 DNS 服务没有强有力的安全机制，一旦被攻击者伪装欺骗，整个网络都有可能遭受攻击。所以在允许的情况下尽量关闭 DNS 服务。关闭 DNS 服务的命令配置如下。

```
Router(config)#no ip domain-lookup
```

关闭 DNS 服务之后，虽然解决了安全威胁，但是依然还有一些 DNS 请求需要被执行，此时可以采用配置手动解析的方法解决这类请求。添加手动解析的命令配置如下。

```
Router(config)#ip host name address1 [address2-address8]
//“name”为需要解析的名字，后面可最多写 8 个对应解析的 IP 地址
```

除此之外，也可以在不关闭 DNS 服务的情况下解决安全问题，即手动配置具体的 DNS 服务器地址，命令配置如下。

```
Router(config)#ip name-server 192.168.100.100
//指定默认使用的 DNS 服务器是 192.168.100.100 主机
```

3. 关闭 HTTP 服务

路由器默认开启了 HTTP 服务，由于访问该服务不需要进行加密认证，所以网络管理员可以很方便的进行连接配置。同样的，网络攻击者也可以利用这个方面修改路由器的 HTTP 配置，以实现攻击。所以为了网络安全，配置路由器时，必须关闭 HTTP 服务。详细命令配置如下。

```
Router(config)#no ip http server
//关闭 HTTP 服务
Router(config)# no ip http secure-server
//关闭 HTTPS 服务
```



HTTPS 服务是加入 SSL 认证的 HTTP 协议，需要一并关掉。

4. 关闭 ICMP 重定向

ICMP 重定向可以将终端节点的 Ping 操作转向特定目标节点。一旦攻击者使用 Ping 命令实施攻击，路由器的 ICMP 重定向功能很可能将该攻击 Ping 发至特定的服务器，攻击者会从中获得服务器的运行状态，并进一步实现攻击。因此网络管理员应该取消远程用户接受 Ping 命令应答功能，禁用 ICMP 协议，这样网管才能更好地防御黑客的扫描。

```
Router(config)#inerface fastethernet0/1
//进入外网接口 fastethernet0/1 的配置子模式
Router(config-if)#no ip redirect
//禁用 ICMP 重定向
```

5. 关闭 IP 源路由选择

IP 协议支持源路由选择，即 IP 报文可以被限定从特定的路由到达目标地址。这主要是用于判断网络的连接故障，用到的几率比较少。但是，一旦使用了该功能，设备就会给攻击者留下一个可攻击的后门，所以需要在全局模式下禁用该服务。具体命令配置如下。

```
Router(config)#no ip source-route
```

12.2.10 启用设备日志记录

设备日志主要用于记录设备运行情况及事件等信息。通过查看日志，网络管理员可以快速找出设备故障原因，或设备运行性能状况等，所以重要的网络设备都应当开启日志功能。

网络设备自身的存储空间比较有限，所以设备日志一般需要配置专门日志服务器进行存放。日志服务器可以选择 Windows 系统下的 Kiwi Syslog 日志软件实现，也可以使用 Linux 系统下的日志服务。

使用 Syslog 记录 Cisco 设备日志，下面介绍设备日志服务的配置方法。

1. 配置设备日志服务

```
Router(config)#logging on
//开启设备的日志服务
```

```
Router(config)#logging 192.168.100.100
Router(config)#logging to host 192.168.100.100 port 514 started
//指定日志服务器的 IP 地址为“192.168.100.100”
Router(config)#logging facility local1
//facility 标识，RFC3164 规定的本地设备标识为 local0~local7，用于和日志服务器的配置文件做匹配
Router(config)#logging trap errors
//日志记录级别，也可用 0~7 表示级别，级别越高表示日志记录信息越详细，如果是 7 代表所有日志都做记录
```

日志级别主要有 8 种，如表 12-1 所示。

表 12-1

级别	名称	级别	名称
	紧急(Emergencies)		警告(Warnings)
	告警(Alerts)		通知(Notifications)
	严重的(Critical)		信息(Informational)
	错误(Errors)		调试(Debugging)

```
Router(config)#logging source-interface e0
//日志发出用的源 IP 地址，可以用端口编号也可以用 IP 地址
Router(config)#service timestamps log datetime localtime
//日志记录的时间戳设置，可根据需要具体配置检验
Router#show logging
//查看日志记录配置信息
```

2. 配置日志服务器

Kiwi Syslog 日志软件可以通过网络获得，免费安装，安装之后默认可以使用，不需要做过多的配置，但是在未注册时，只能记录一个设备的日志信息，并且 Kiwi Syslog 日志软件应用于 Windows 环境下，安全隐患较多。一般建议选择在 Linux 环境下搭建日志服务器。

在 Linux 环境下搭建日志服务器的配置方法如下。

（1）修改远程服务器配置文件

```
vi /etc/sysconfig/syslog
```

将“SYSLOGD_OPTIONS="-m 0"”改为“SYSLOGD_OPTIONS="-r -m 0"”，其中“-r”代表允许从远程主机写入。

（2）配置本地日志主配置文件

```
vi /etc/syslog.conf
```

加入“local1.* /var/log/router.log”行，“local1”是设备标识要和设备日志配置里的标示匹配，“*”匹配所有日志级别，“/var/log/router.log”为存放日志记录的日志文件。

（3）生成空的日志文件

```
touch /var/log/router.log
```

（4）重启 syslog 服务

```
/etc/rc.d/init.d/syslog restart
```

或使用以下命令：

```
service syslog restart
```



日志服务使用的默认端口为 UDP/514、TCP/146，在配置访问控制策略时不要误将这些流量过滤掉。

配置网络设备的日志服务是很重要的，但是只做记录而不去查看，那么日志服务的配置就没有任何意义了。通常网络管理员可用使用 webadmin 工具管理和查看日志，同时还可以使用 logchek 命令将有问题的日志筛选出来，以做分析。

12.2.11 设置广播风暴抑制比

在网络中存在有大量的广播数据包，这些数据包一方面是网络正常连接所必须的，但另一方面也很容易被病毒或网络攻击所利用。计算机、路由器、交换机等所有网络中的设备，都会对广播数据包进行相应的处理，如果广播流量过大，这些设备就必须提供一定的性能资源浪费在处理这些广播数据包上。同时，广播数据包过多也会极大地占用网络带宽资源。所以，广播流量的增大会影响整个网络的性能及应用。所以在网络环境下，需要对广播数据包进行合理的限制。

为了必要广播数据包的通信，一般不会完全限制广播流量。使用比较多的方法有缩小广播域，可以通过增加设备或 VLAN 划分的方式减小广播域内的主机数量，但是这种方法可能需要增添新设备。除此之外，还可以通过设定广播抑制比的方式。通过命令限制指定端口上允许通过的广播流量，当广播流量过多超出限定范围时，会采取丢弃操作，这样就可以将广播流量限制在可控的范围内，避免网络性能的浪费。下面以交换机为例介绍广播风暴抑制比的详细配置。

1. 抑制带宽百分比

可以通过广播流量占用整个带宽的百分比进行限定，当达到指定的百分比时，自动抑制广播流量，当广播流量达到下限值时取消限制，不过下限值一般采用默认配置。默认广播风暴抑制比配置为 100%，表示广播风暴抑制比被关闭，允许所有广播流量通过，直至带宽耗尽。如果限制所有广播流量通过，可以将值设为 0%。

一般建议配置 10%~30%。以 20%为例，具体配置命令如下。

```
Switch#configure terminal
//进入全局配置模式
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 接口的配置子模式
Switch(config-if)#storm-control broadcast level 20
//设定广播流量的抑制比为 20%，超过总带宽 20%的流量丢弃
```

2. 抑制单位时间广播包

也可以通过单位时间内统计的广播数据包的值实现广播抑制，一般会设定两个值，上限值和下限值。当达到上限时，开始阻止广播包转发，当流量低于下限值时，取消限制。

值的设定要根据网络环境下的主机数量。具体配置命令如下。

```
Switch(config-if)#storm-control broadcast level pps 50 20
//设定每秒允许通过的广播数据包上限为 50 个，下限值为 20 个
```

12.2.12 关闭路由器广播包转发

一般路由器会隔离广播域，阻止转发广播数据包，但是碍于应用需求，还有一些网络设备开启了路由器的广播转发功能。因此，一些网络攻击就以路由器广播转发的配置为跳板实施网络攻击，比如 SumrfDos 攻击。攻击实现后会占用网络资源，甚至导致网络设备瘫痪，所以要在路由器的每个端口上关闭路由器的广播包转发功能。具体配置命令如下。

```
Switch(config)#interface fastEthernet 0/1
//进入 fastEthernet 0/1 接口的配置子模式
Switch(config-if)# noipdirected-broadcast
//关闭广播包转发功能
```

12.3 专家答疑

（1）使用其他品牌的网络设备是否具有相同的安全问题？

答：本章列举的网络安全问题并不是全部，只是比较常见的安全问题，不过也有一些是 Cisco 专有的技术，如 CDP（Cisco 发现协议），很多设备就不支持。网络厂商比较多，不同的厂商设备差异很大，特别是生产研发体系不健全的厂商，产品的安全漏洞问题可能更多。所以无论是哪一款设备，在实施网络安全之前，都需要先对设备进行一个深入的了解，也可和通用的网络设备安全配置做比较，判断其是否具有该安全隐患。

（2）如果某台设备的系统镜像本身存在漏洞怎么办？

答：设备在出厂时自带的系统镜像可能会存在一些漏洞，这些漏洞有时不是更改服务就可以修复的。为此，各厂商也会对自己的产品做检查、升级，而且升级的补丁包和方法都会对外发布，用户可以结合设备的情况，去厂商官网查找最新更新的系统镜像或者补丁。不同设备的更新方法不同，可以在其官方网站获得。

如果设备本身没有发现异常，但是厂商给出了新的更新程序，也不一定非要更新，用户一定要先确认更新是否稳定，且没有新的漏洞。这些信息可以去各厂商论坛查询。

第 13 章　无线网络安全管理

随着网络的发展，人们对网络的要求越来越高，需要随时随地的访问互联网，无线网络就应运而生了。无线网络是利用无线电波来作为数据传输的媒介，就应用层面而言，与有线网络的用途完全相似，最大的不同是传输信息的媒介不同。

13.1　无线网络现状

随着无线局域网的标准日趋完善，相关的技术和产品逐渐在市场上推广开来，近年来无线网络在国内外逐渐流行。目前，无线局域网已经具有一定的速度和可靠性，可以提供优质的无线移动服务。

13.1.1　便捷的应用

随着笔记本、具有 WIFI 功能的手机、PDA（个人数字助理）等无线客户端的流行，无线网络越来越受到人们的青睐。无线网络的特征是以一个固定的信息点为基础，形成一个网络覆盖面。对于无线终端用户来说，只要无线网卡能搜索到无线信号，就可以随时随地的访问互联网，无线网络带来的便捷性不言而喻。

1. 免去布线的麻烦

传统的计算机使用网线连接至互联网，但是很多时候受到房间等各种原因的限制，线缆不能连接，比如外租房，大部分房东不愿意在屋内凿洞拉线，这时候上网就成了问题。如果采用无线网络，只需要在 ISP 运营商接口连接一根线缆至屋内无线路由器上，无线客户端不需要线缆也可以直接连接至互联网。

2. 减少投资

无线网络没了线缆的连接，就减少了线缆和施工的费用，只要购买性能良好的无线 AP 即可，可以节约很大的成本。

3. 随时随地上网

随着无线校园、无线城市的兴起，使得人们可以在无线校园、无线城市内部随时随地上网，不需要受到没有网线的限制。

13.1.2 可怕的隐患

无线网络技术在给人们带来便捷的同时，也给用户带来了一定的安全风险。无线网络是靠无线信号传输数据，无线信号在被无线 AP 发射出去之后，无线信号的传输路径是无法被控制的，因此，无线信号很容易被陌生的接收者接收到，除非在无线 AP 处设置了足够安全的访问者及无线客户端设备的身份验证和授权机制，否则任何具有兼容功能的无线客户端或者用户都可以接受该网络的数据。

1. 追求无线 AP 覆盖面过大带来的安全隐患

无线 AP 都有一定的发射功率，发射功率决定了无线网络的覆盖范围，很多人为了方便，过度追求无线网络的覆盖范围，就购买大量的或者大功率的无线 AP，这样只会让更多的无线客户端扫描到无线网络，无形中会增加无线网络受到攻击的几率。因此，不要一味地追求无线网络的覆盖范围，只要满足需求就可以。另外，从安全角度考虑，无线 AP 的放置位置也较为重要，一般情况将无线 AP 放置在无线网络中央，避免将无线 AP 放在离窗口过近的地方，这样无线信号外泄的机会会减少。

2. 无线 AP 数据传输没有加密带来的安全隐患

很多人在购买无线路由器后，根据无线路由器设置说明进行设置后，直接利用无线路由器进行上网，而没有对无线路由器的默认出厂设置进行任何更改，更没有对无线网络的数据传输的加密机制进行设置。在这种情况下，无线网络的安全问题最容易发生。

3. 无线网络破解工具的流行带来的安全隐患

随着无线网络的流行，各种无线破解技术也开始在市场上出现，因此即使对无线 AP 进行了严格的安全措施，比如加大无线 AP 管理员的密码复杂度、设置无线 AP 数据加密等，也有可能会被无线网络破解工具破解。

13.2 无线安全实施措施

人们在享受无线网络带来便捷性的同时，必须时刻注意无线网络的安全性，因为无线网络的信号总是以广播的形式在传输，具备无线扫描功能的任何设备都能随时随地接收到区域内的无线信号，这时就需要在无线 AP 处设置无线客户端的准入机制或数据加密工作，防止未被授权的设备登录无线 AP。

13.2.1 家庭无线局域网的管理

随着计算机的普及，更多的家庭拥有了不止一台计算机，于是便产生了家庭局域网。家庭局域网最开始是选择购买家用路由器，然后进行网线的连接。但在方便共享上网的同时，蜘蛛网般的网线连接影响了家庭的整体美观，于是人们开始追求家庭无线局域网，没有网线的束缚却能享受有线网络的乐趣。

下面详细介绍如何建立家庭无线网络，需要准备的硬件是家用无线路由器，本实例以 TP-LINK TL-WR340G+ 54M 型号无线路由器进行讲解，然后进行线缆的连接，如图 13-1 所示为家用无线路由器的连接拓扑图。

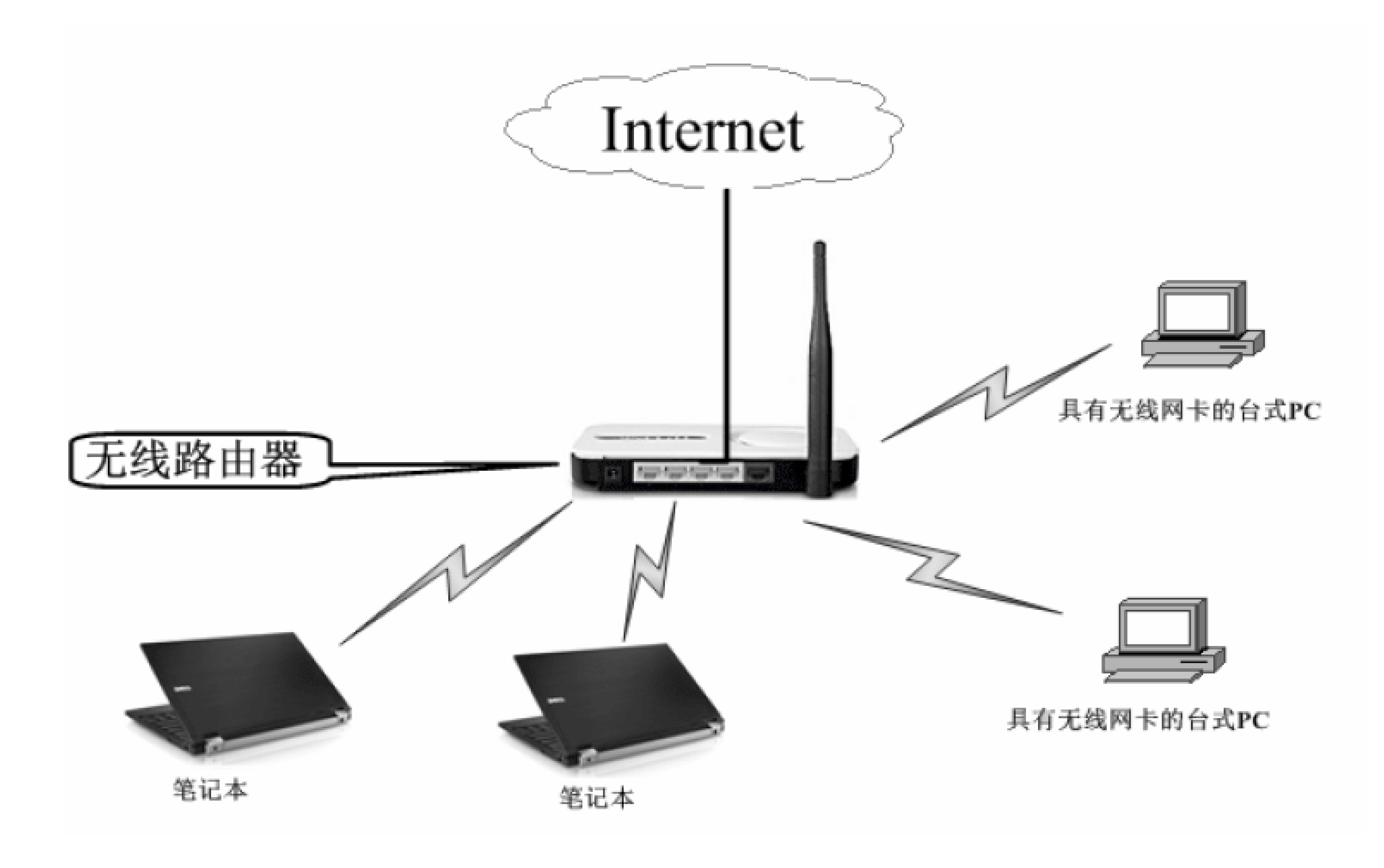


图 13-1

1. 开启路由器无线功能

建立家庭无线局域网的第一步是开启路由器无线功能，具体的操作步骤如下。

01 本机的 IP 地址设置为 192.168.1.0/24 网段，然后在 IE 浏览器的地址栏中输入 http://192.168.1.1，如图 13-2 所示，单击【转到】按钮。

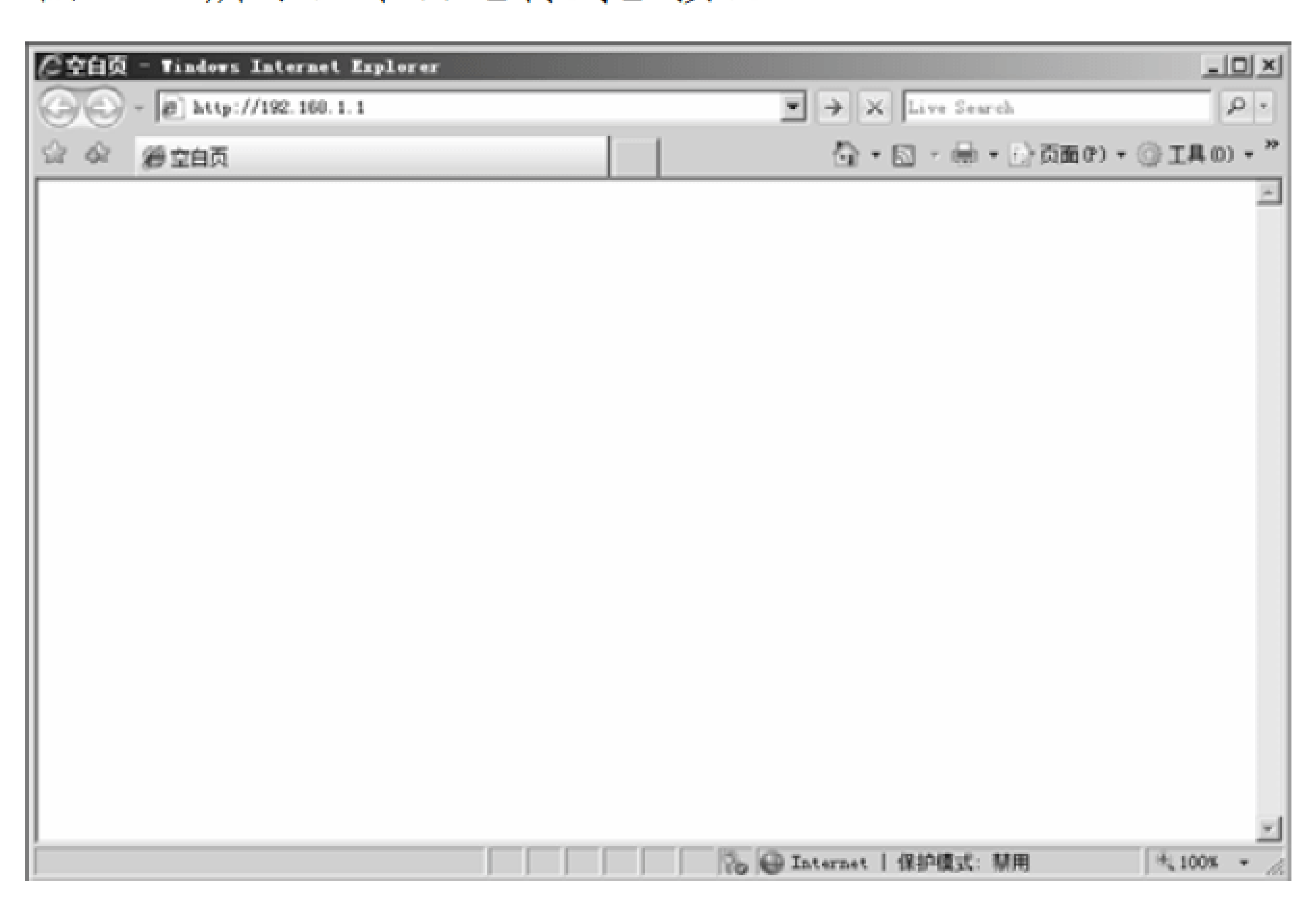


图 13-2



IP 地址设置哪个网段以及用什么 IP 地址访问路由器，具体需要参考《无线路由器使用操作说明书》，不过大部分的 TP-LINK 路由器默认 IP 地址都为 192.168.1.1。

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，如图 13-3 所示，单击【确定】按钮。

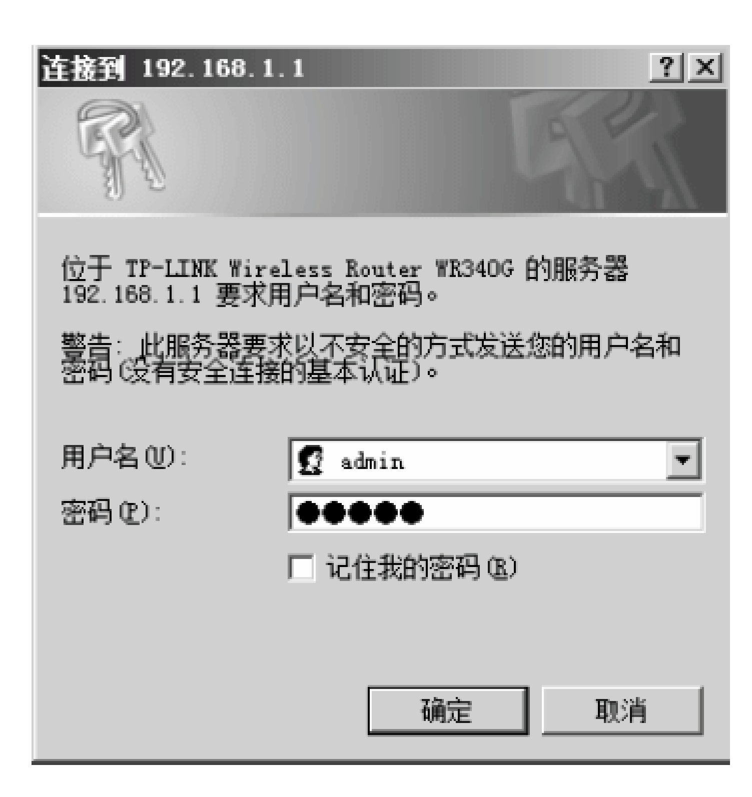


图 13-3

03 弹出【TP-LINK】路由器的设置页面，选择左侧【网络参数】➢【WAN 口设置】选项，设置 TP-LINK 的上网方式。在【WAN 口连接类型】下拉菜单中选择上网方式，一般情况下家庭都是通过 ADSL 方式也就是电话线上网，需要在【WAN 口连接类型】下拉列表中选择【PPPoE】选项，在【上网账号】和【上网口令】文本框中分别输入合法的上网账号和密码，如图 13-4 所示，单击【连接】按钮即可。



图 13-4

04 选择左侧【网络参数】➢【LAN 口设置】选项，在【IP 地址】和【子网掩码】文本框中分别输入局域网内部计算机的网关和子网掩码，需要注意这个 IP 地址就是内部局域网计算机的网关，同时也是客户机访问 TP-LINK 路由器的 IP 地址，本实例中输入“192.168.1.1”，如图 13-5 所示，单击【保存】按钮即可。

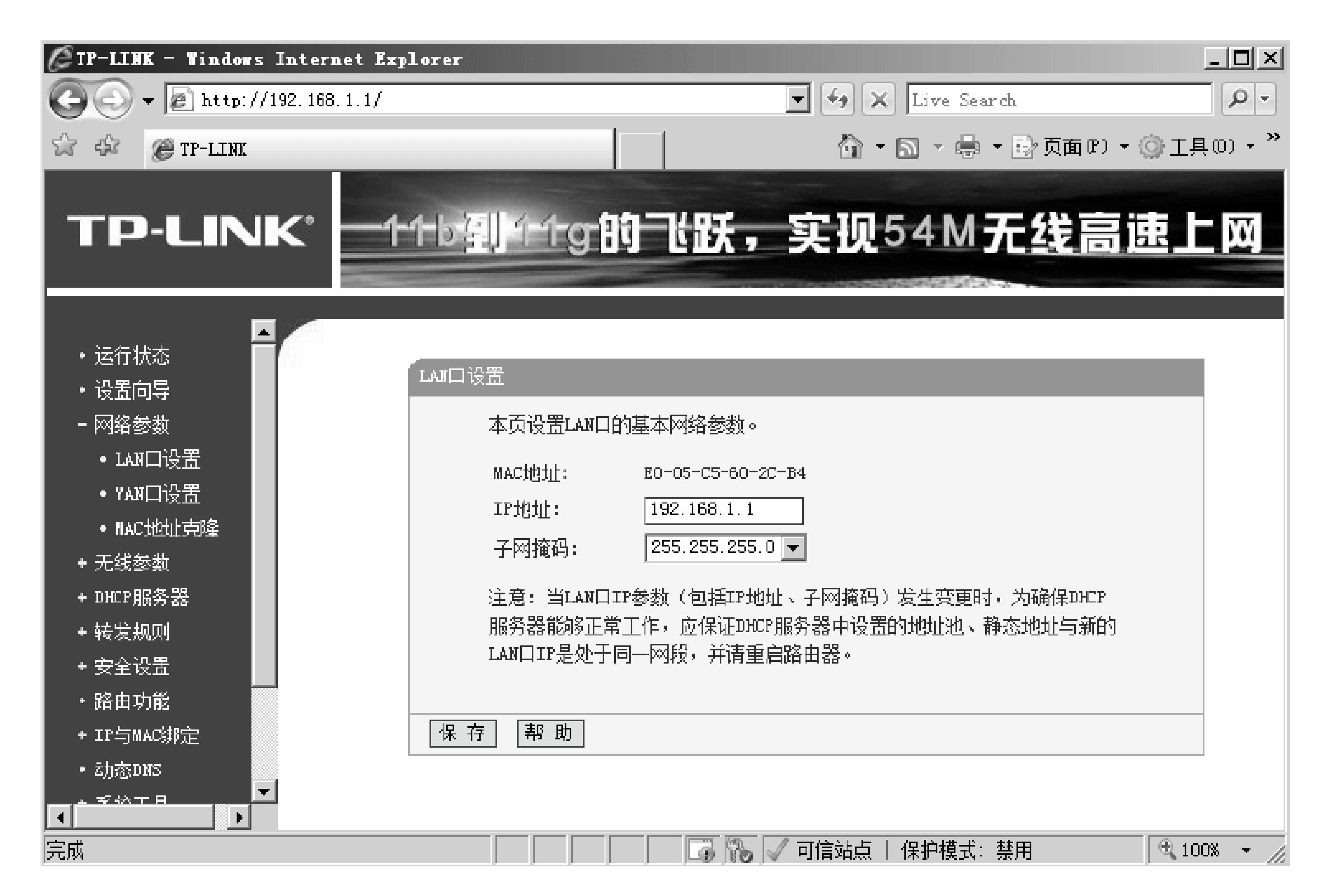


图 13-5

05 选择左侧【无线参数】➢【基本设置】选项，选择【开启无线功能】复选框，如图 13-6 所示，单击【保存】按钮，到此一个简单的无线路由器就设置完毕。

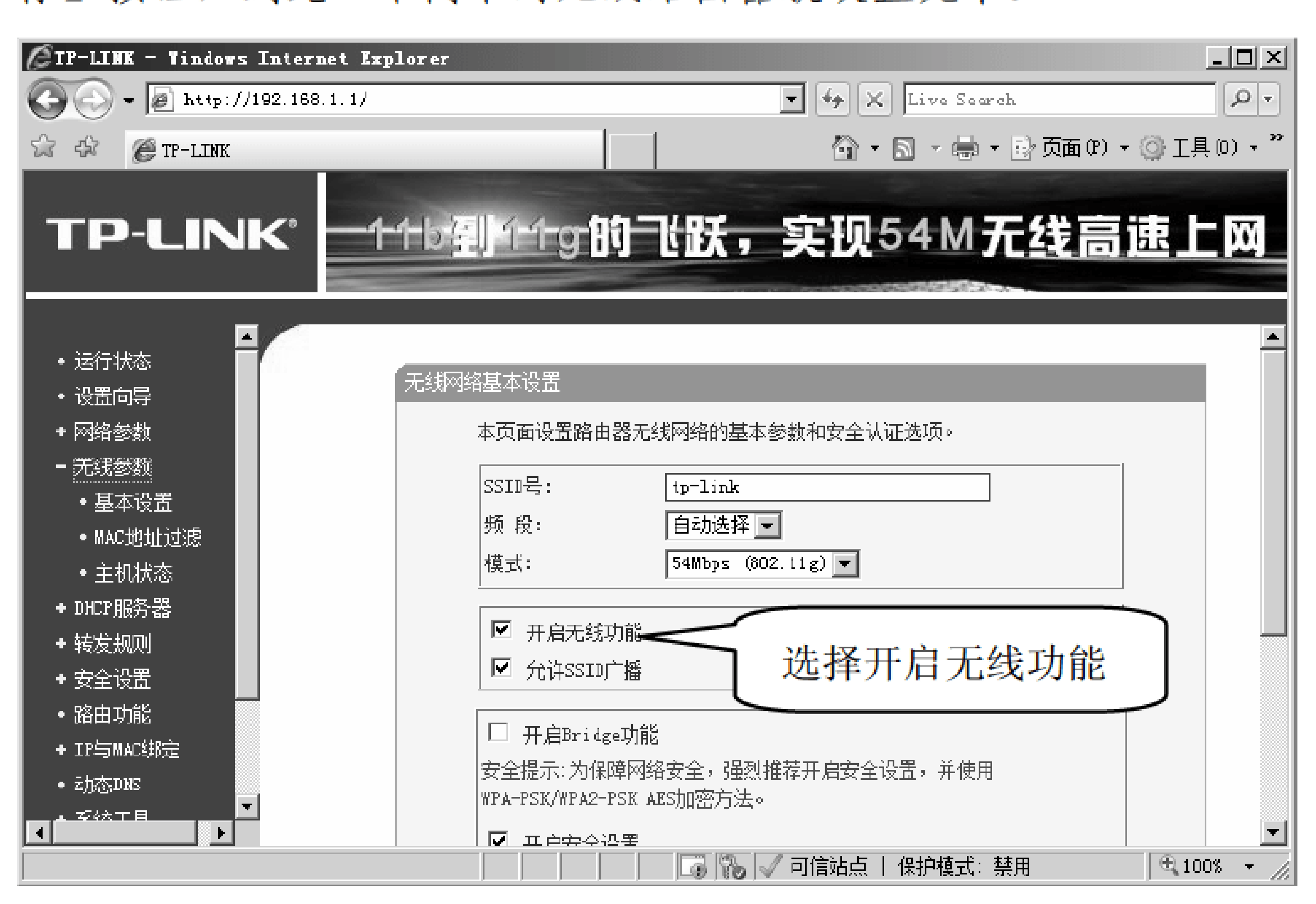


图 13-6

2. 客户端连接

建立家庭无线局域网的第二步是连接无线客户端，具体操作步骤如下。

01 客户端连接无线路由器。本实例采用 Win7 系统的笔记本来作为无线客户端。单击系统桌面右下角的【】图标，如图 13-7 所示，会看到无线客户端自动扫描到区域内的所有无线信号。



图 13-7

02 右击扫描出现的【tp-link】信号，在弹出的快捷菜单中选择【连接】选项，如图 13-8 所示。



图 13-8

03 连接成功后，在系统右下角出现【】图标，将鼠标放在【tp-link】信号上面，可以看到该无线信号信息，如图 13-9 所示。此时，该计算机就可以正常的访问互联网了。



图 13-9

13.2.2 无线安全加密

无线网络不需要物理线缆，非常方便，但正因为无线网络需要靠无线信号进行信息传输，而无线信号又管理不便，因此，数据的安全性遭遇了前所未有的挑战，于是，各种各样的无线加密算法应运而生。

1. WEP 加密

相对于有线网络来说，通过无线局域网发送和接收数据更容易被窃听。设计一个完善的无线局域网系统，加密和认证是需要考虑的两个必不可少的安全因素。无线局域网中应用加密和认证技术的最根本目的就是使无线业务能够达到与有线业务同样的安全等级。针对这个目标，IEEE802.11 标准中采用了 WEP(Wired Equivalent Privacy:有线对等保密)协议来设置专门的安全机制，进行业务流的加密和节点的认证。它主要用于无线局域网中链路层信息数据的保密。

WEP 采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。WEP 使用加密密钥(也称为 WEP 密钥)加密 802.11 网络上交换的每个数据包的数据部分。启用加密后，两个 802.11 设备要进行通信，必须具有相同的加密密钥，并且均配置为使用加密。如果配置一个设备使用加密而另一个设备没有，则即使两个设备具有相同的加密密钥也无法通信。也就是说所有无线客户端和无线接入点必须使用一个共享的加密密钥进行加密，密钥越长，黑客破解的时间越长，也就越安全。

下面详细介绍无线网络 WEP 加密的具体方法。

（1）设置无线路由器 WEP 加密数据

设置无线路由器 WEP 加密数据具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，访问无线路由器，如图 13-10 所示，单击【转到】按钮。

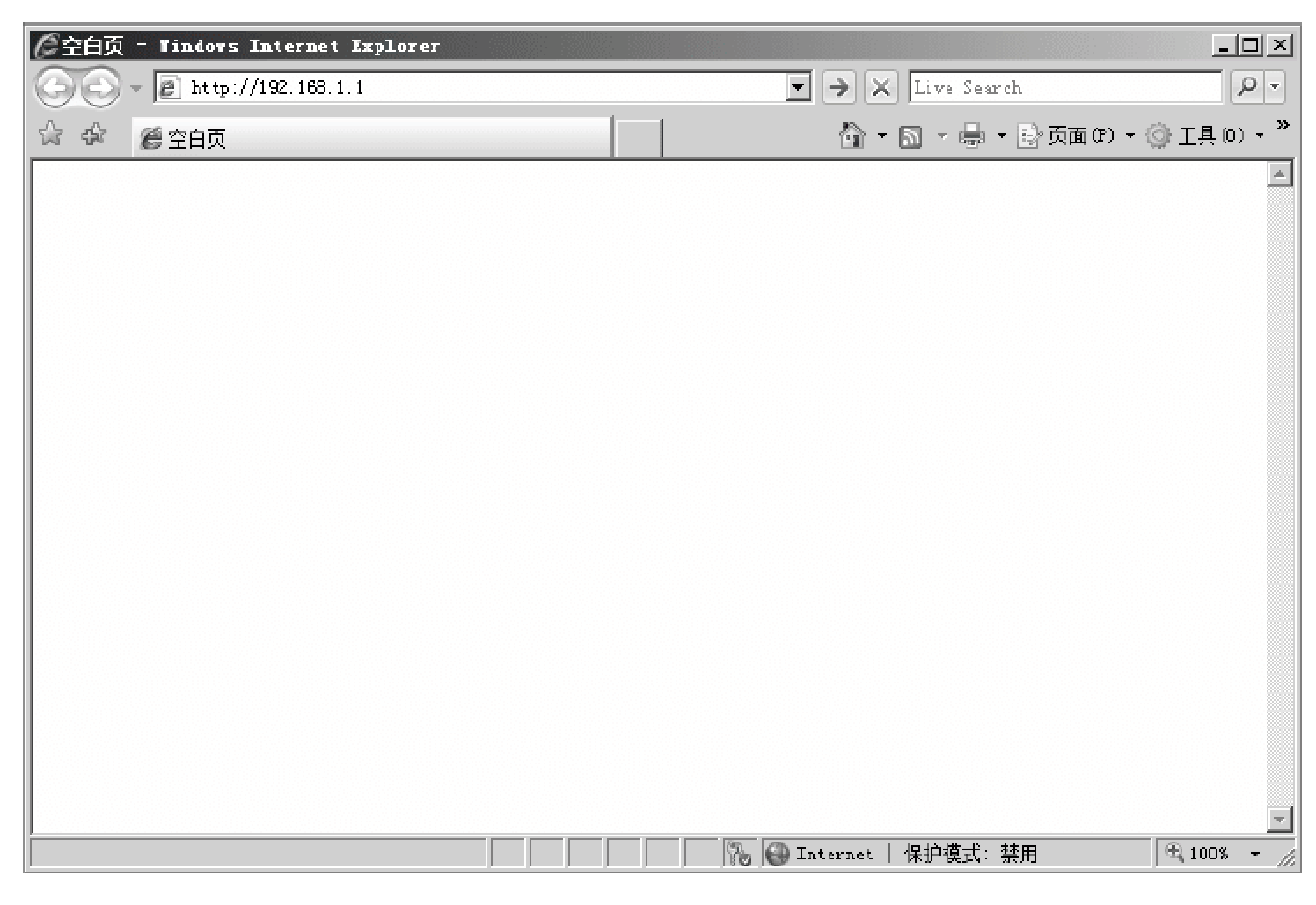


图 13-10

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 家用路由器的默认用户名和密码都为“admin”，如图 13-11 所示，单击【确定】

按钮。

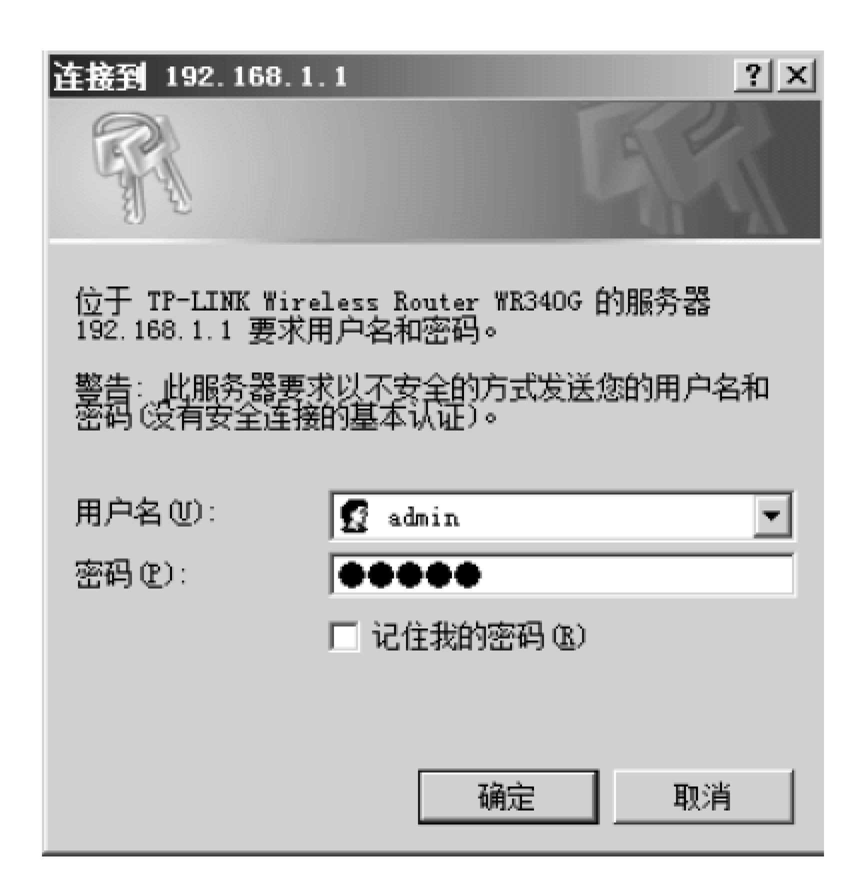


图 13-11

03 单击左侧【无线参数】➢【基本设置】选项，选择【开启安全设置】复选框，在【安全类型】下拉菜单中选择【WEP】选项，在【密钥格式选择】下拉菜单中选择【ASCⅡ码】选项。设置密钥，在【密钥 1】后面的【密钥类型】下拉列表中选择【64 位】选项，在【密钥内容】文本框中输入要使用的密码，本实例输入密码为“cisco”，单击【保存】按钮，如图 13-12 所示。

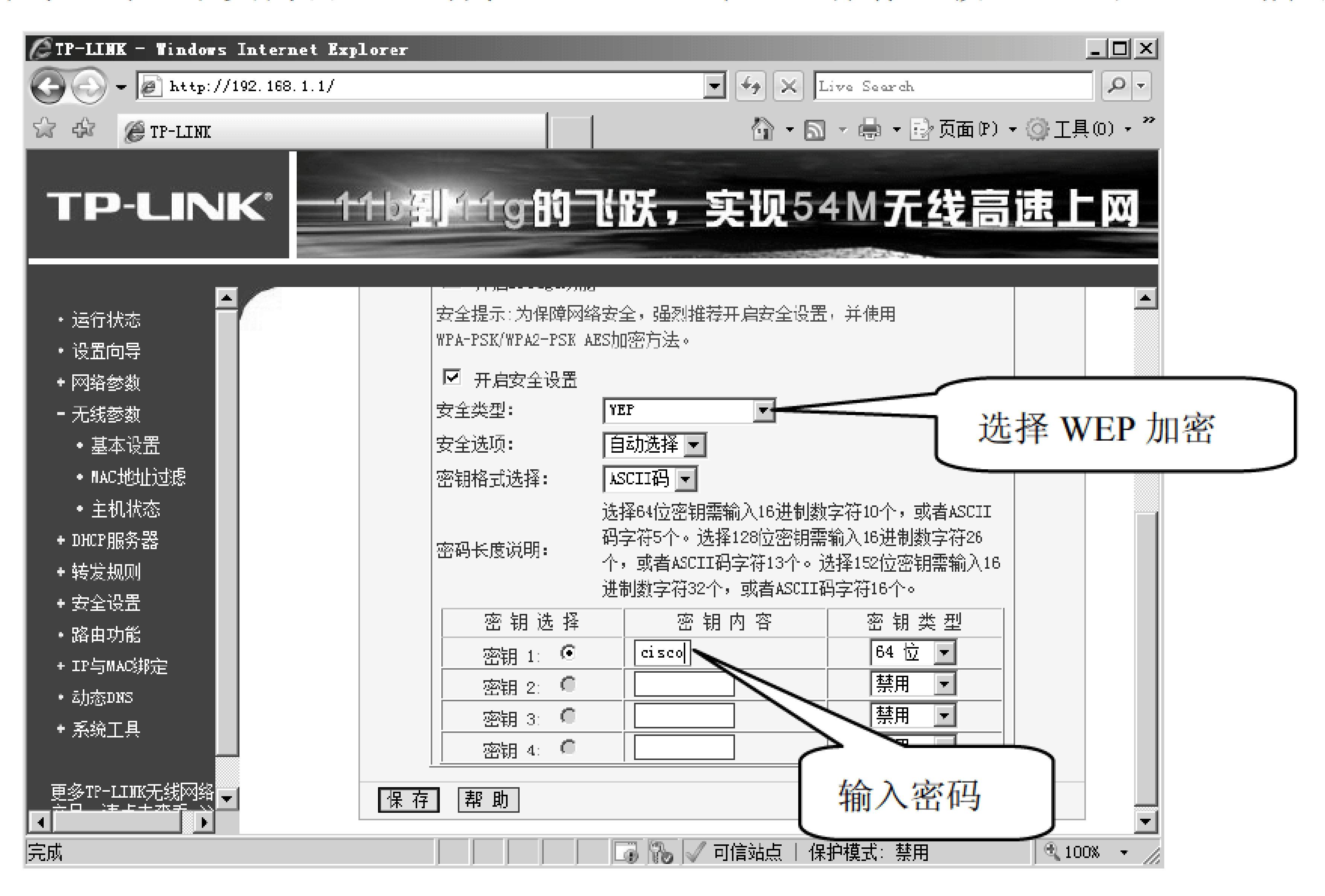


图 13-12

（2）客户端连接

需要 WEP 加密认证的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角【】图标，无线客户端自动扫描到区域内的所有无线信号，如图 13-13 所示。

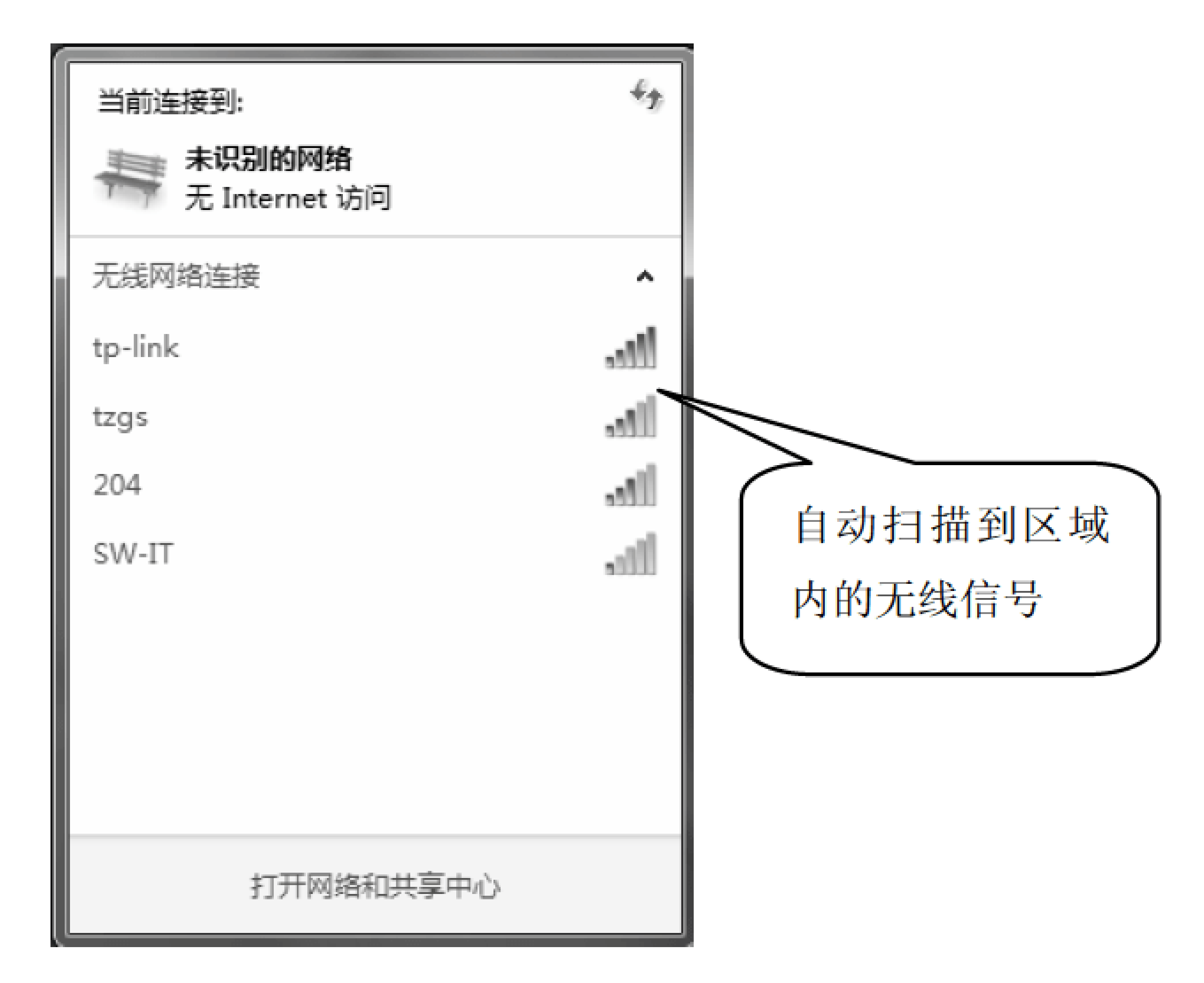


图 13-13

02 右击【tp-link】信号，在弹出的快捷菜单中选择【连接】选项，如图 13-14 所示。



图 13-14

03 弹出【连接到网络】对话框，在【安全密钥】文本框中输入密码“cisco”，单击【确定】按钮，如图 13-15 所示。



图 13-15

04 单击系统桌面右下角【】图标，将鼠标放在【tp-link】信号上，可以看到无线信号的连接情况，如图 13-16 所示，表明已经成功连接无线路由器。



图 13-16

2. WPA 加密

早期的 WEP 无线加密算法在无线网络的数据安全方向起到了很大的作用，但是 WEP 使用的是静态的密钥而非动态密钥，导致 WEP 密码很容易被监听到或者破解，因此，在组建无线网络的时候，理想的做法是用 WPA 和 WPA2 加密算法来代替 WEP。

WPA 算法主要用于增强无线局域网系统的数据保护和访问控制水平，采用了动态的加密密钥。WPA2 是在 WPA 的基础之上，经由 Wi-Fi 联盟验证过的 IEEE802.11i 标准的验证形式，是目前公认的比较安全的无线加密算法。

WPA 作为 WEP 的升级版，在安全性方面有了很大的改进，主要体现在身份验证、加密机制和数据包检查等方面，并且 WPA 使用了动态密钥，使得黑客破解起来相当费力。但是完整的 WPA 设置比较复杂，一般用户很难操作，导致 WPA 和 WPA2 算法在实际中应用很少，除非是对无线网络要求及其苛刻的公司才会使用。

3. WPA-PSK 安全加密算法

由于 WPA 操作复杂，因此不管是在家庭还是在公司的应用中经常采用 WPA 的简化版：WPA-PSK 和 WPA2-PSK。WPA-PSK 可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（例如无线路由器），只要密码正确，就可以使用无线网络。

WPA-PSK 安全加密机制和 WPA 是相同的，两者的区别是：WPA-PSK 认证被简化为只要一个简单的密码，而不需要设置复杂的身份证明等信息。WPA-PSK 的缺点是：同 WEP 一样也易受到黑客的破解。但因为密钥是动态的，其安全性比 WEP 要强很多。

下面介绍如何使用 WPA-PSK 或者 WPA2-PSK 加密无线网络的方法。

（1）设置无线路由器 WPA-PSK 安全加密数据

设置无线路由器 WPA-PSK 安全加密的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，如图 13-17 所示，单击【转到】按钮。

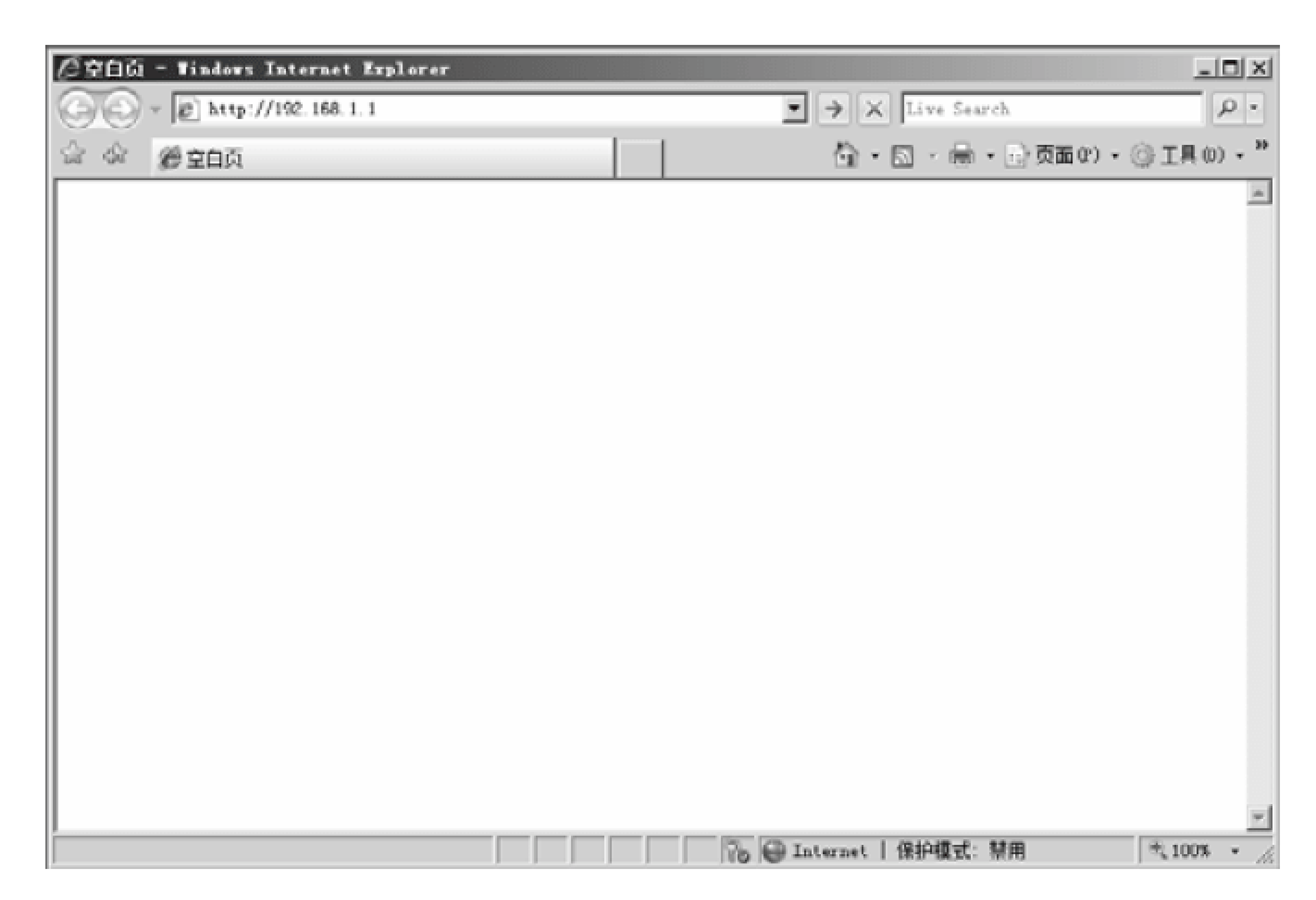


图 13-17

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP－LINK 的家用路由器的默认用户名和密码都为“admin”，如图 13-18 所示，单击【确定】按钮。

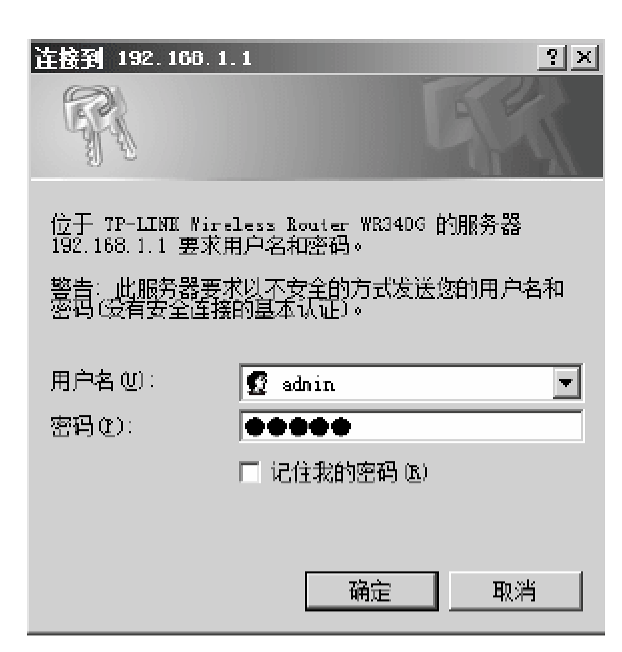


图 13-18

03 选择左侧【无线参数】➢【基本设置】选项，选择【开启安全设置】复选框，在【安全类型】下拉列表中选择【WPA-PSK/WPA2-PSK】选项，在【安全选项】和【加密方法】下拉菜单中分别选择【自动选择】选项，在【PSK 密码】文本框中输入加密密码，本实例设置密码为“sushi1986”，如图 13-19 所示，单击【保存】按钮。

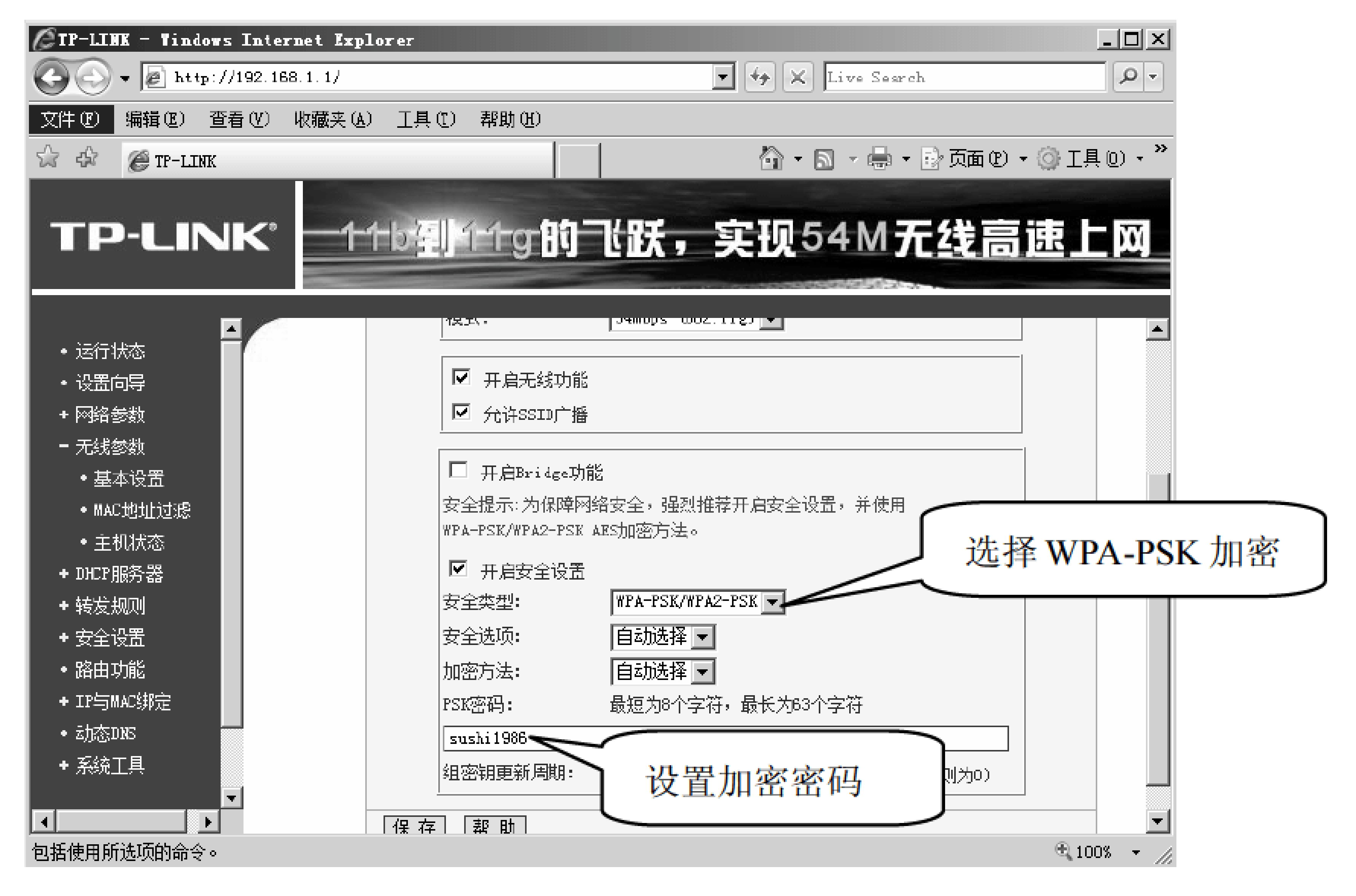


图 13-19

04 弹出【Windows Internet Explorer】提示对话框，如图 13-20 所示，单击【确定】按钮，重新启动路由器即可。

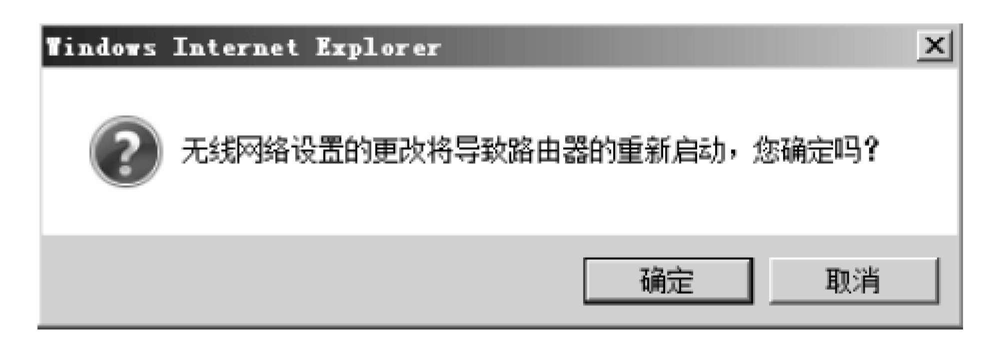


图 13-20

（2）客户端连接

使用 WPA-PSK 安全加密认证的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角【】图标，无线客户端会自动扫描区域内的无线信号，如图 13-21 所示。

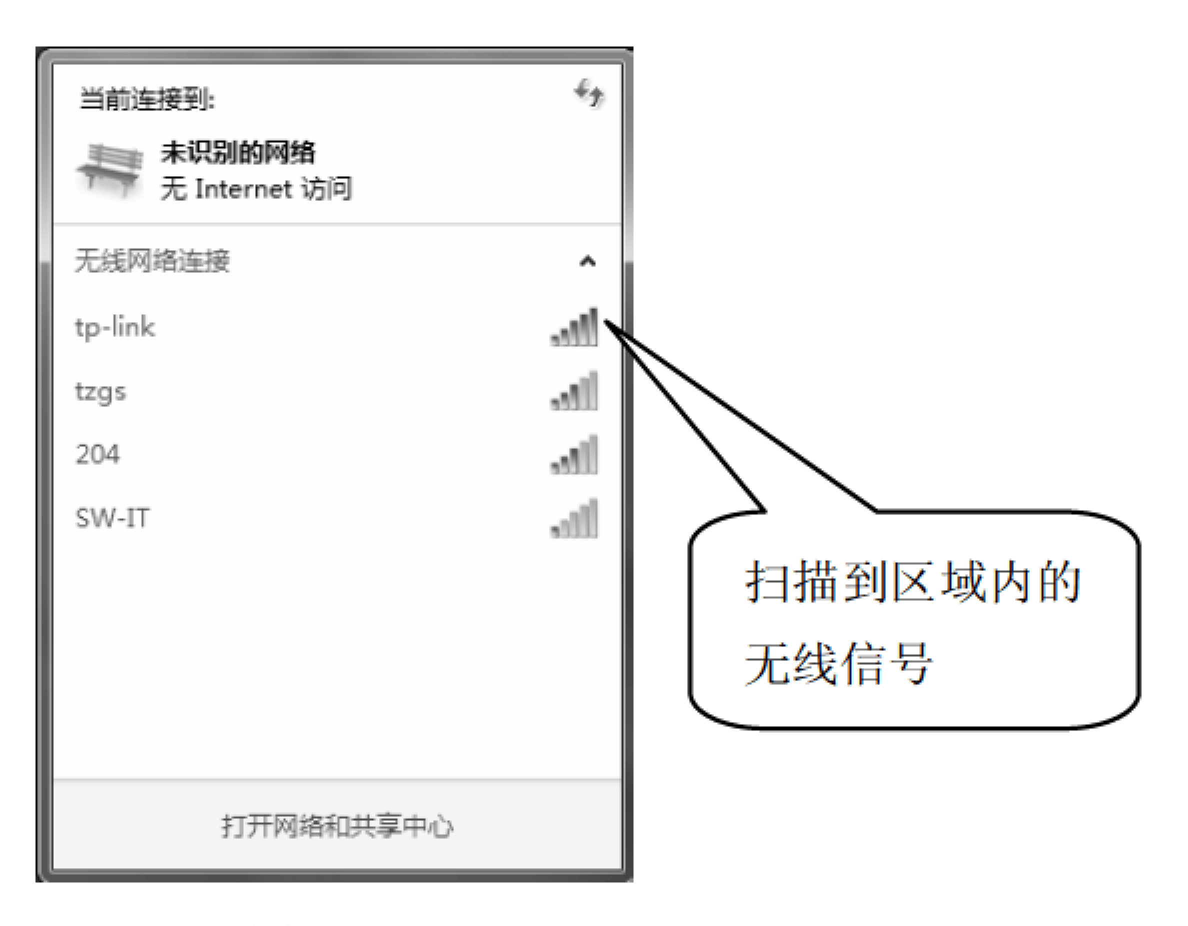


图 13-21

02 右击【tp-link】信号，在弹出的快捷菜单中选择【连接】菜单命令，如图 13-22 所示。



图 13-22

03 弹出【连接到网络】对话框，在【安全密钥】文本框中输入密码“sushi1986”，单击【确定】按钮，如图 13-23 所示。



图 13-23

04 单击系统桌面右下角【】图标，将鼠标放在【tp-link】信号上，可以看到无线信号的连接情况，如图 13-24 所示，表明已经成功连接无线路由器。



图 13-24



在 WPA-PSK 加密算法的使用过程中，密码设置应该尽可能复杂，并且要注意定期更改密码。

13.2.3 设置独特的 SSID

SSID（Service Set Identifier）主要用来区分不同的无线网络，相当于给每个无线网络设置了 ID 号码，只有当无线客户端和无线 AP 的 SSID 一样时，才可以进行通信。一般情况下，无线网络的 SSID 在无线 AP 上进行设置并有 AP 广播出来，经过无线客户端的扫描功能可以看到当前区域的无线网络，然后选择相应的 SSID 进行连接。因此 SSID 就相当于是无线网络的名称，一般情况下将 SSID 设置为具有独特意义的字符，比如说公司的名称等。

下面介绍如何设置 SSID 的具体操作步骤。

1. 设置无线路由器独特的 SSID

设置无线路由器独特的 SSID 的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，如图 13-25 所示，单击【转到】按钮。

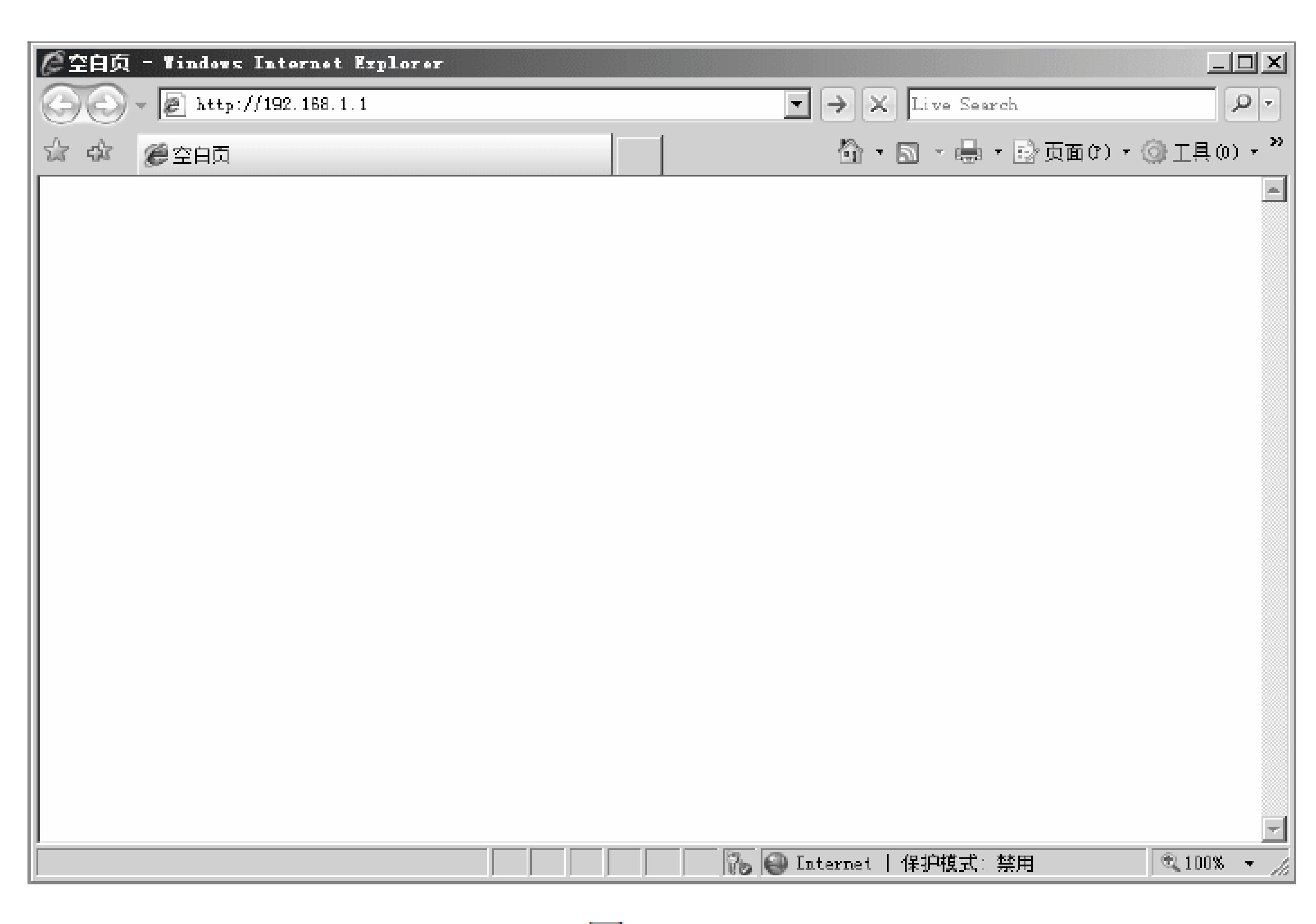


图 13-25

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，如图 13-26 所示，单击【确定】按钮。



图 13-26

03 单击左侧【无线参数】➢【基本设置】选项，选择【开启安全设置】复选框，在【SSID 号】文本框中输入要设置的 SSID 号，本实例输入 SSID 号为“ssh”。在【频段】下拉列表中选择要使用的频段，在【模式】下拉列表中选择要使用的无线网络协议，如图 13-27 所示，单击【保存】按钮。



图 13-27



提 示

频段可以任意选择，但是在一个区域内多个 SSID 的频段不能重复，在选择模式时，如果选择 802.11g 协议则无线网络的速度最快可以达到 54Mbps，如果选择 802.11b 协议则无线网络的最快速度可以达到 11Mbps，要注意的是，无线路由器采用什么协议需要无线客户端的支持。

04 弹出【Windows Internet Explorer】提示对话框，如图 13-28 所示，单击【确定】按钮，重新启动路由器即可。



图 13-28

2. 客户端连接

使用 SSID 设置的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角【】图标，会看到无线客户端自动扫描到区域内的所有无线信号，在其中看到的信号名称 “ssh” 就是刚才设置的无线网络的 SSID，如图 13-29 所示。

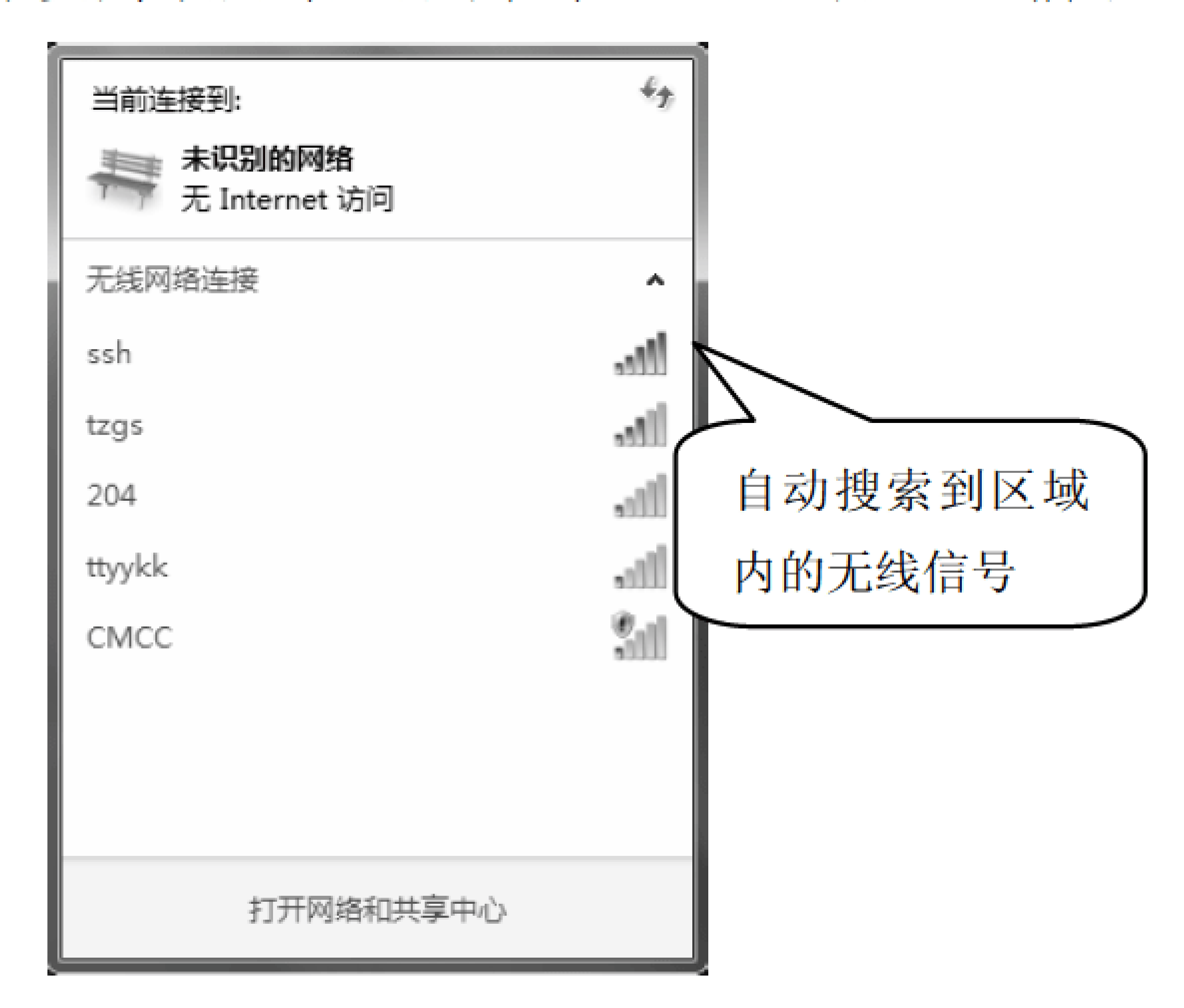


图 13-29

02 右击无线信号【ssh】，在弹出的快捷菜单中选择【连接】选项，如图 13-30 所示。



图 13-30

03 弹出【连接到网络】对话框，在【安全密钥】文本框中输入安全密钥 “sushi1986” ，如

图 13-31 所示，单击【确定】按钮。



图 13-31

04 单击系统桌面右下角【】图标，将鼠标放在无线网络【ssh】上可以看到无线网络的连接情况，如图 13-32 所示无线客户端已经成功连接到无线路由器。



图 13-32

13.2.4 禁用 SSID 广播

SSID 就是一个无线网络的名称，无线客户端通过无线网络的 SSID 来区分不同的无线网路。为了安全起见，往往要求无线 AP 禁止广播该 SSID，只有知道该无线网络 SSID 的人员才可以进行无线网络连接，禁用 SSID 广播的具体操作步骤如下。

1. 设置无线路由器禁用 SSID 广播

无线路由器禁用 SSID 广播的具体操作步骤如下。

01 IE 浏览器的地址栏中输入“http://192.168.1.1”，如图 13-33 所示，单击【转到】按钮。

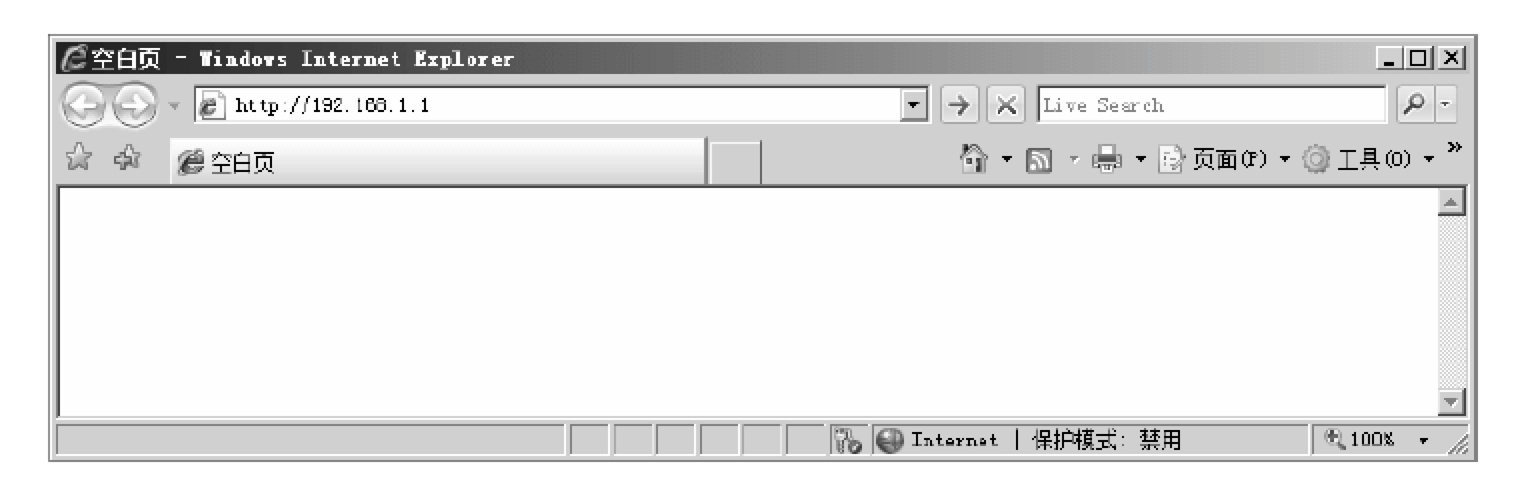


图 13-33

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，如图 13-34 所示，单击【确定】按钮。

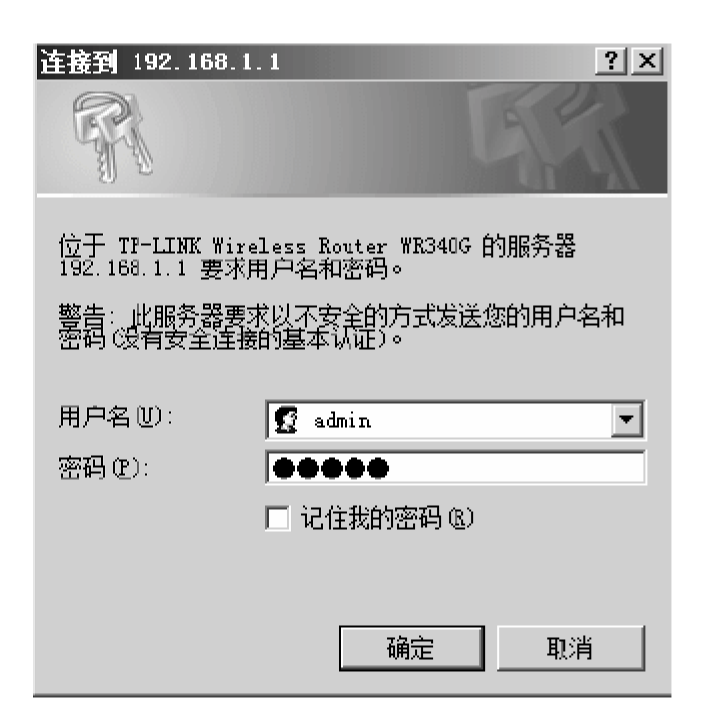


图 13-34

03 设置自己无线网络的 SSID 信息，取消选择【允许 SSID 广播】复选框，如图 13-35 所示，单击【保存】按钮。

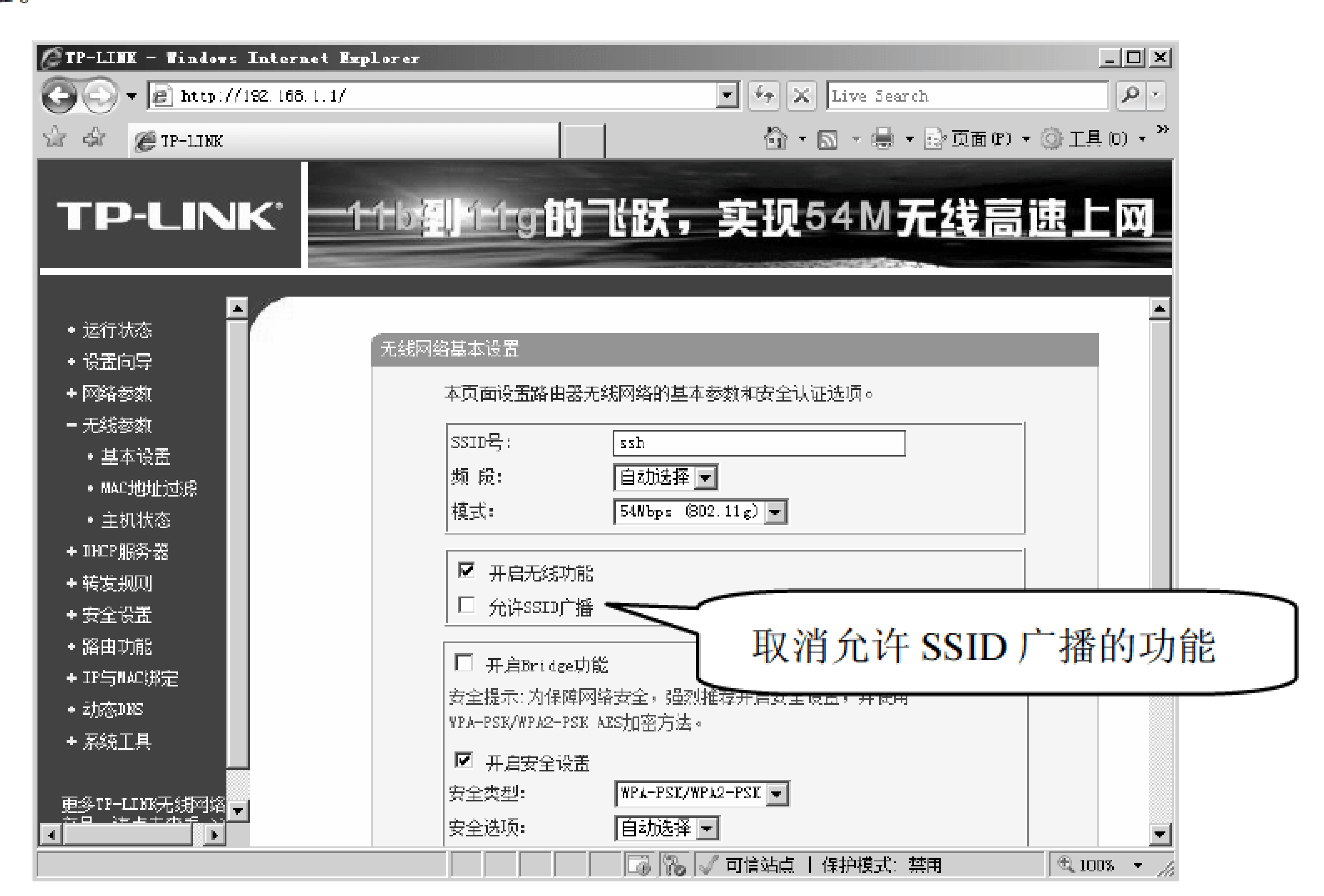


图 13-35

04 弹出【Windows Internet Explorer】提示对话框，如图 13-36 所示，单击【确定】按钮，重新启动路由器。

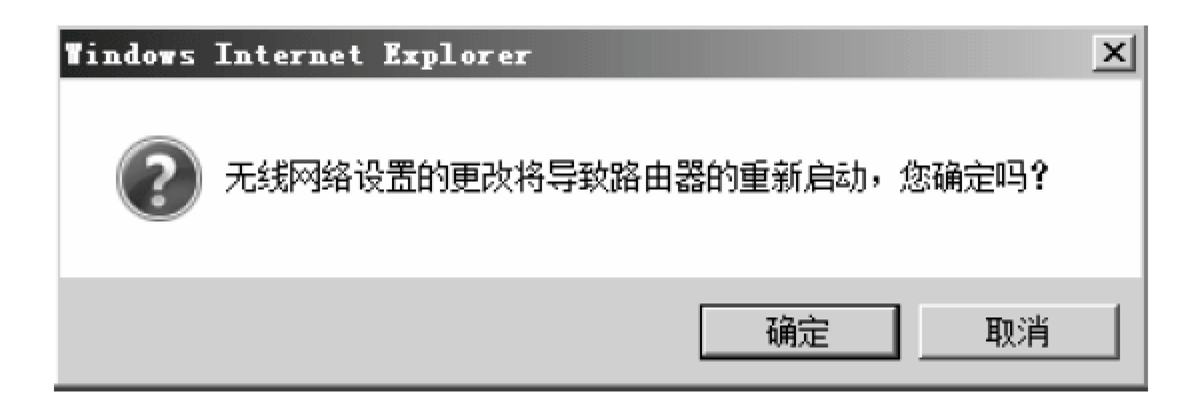


图 13-36

2. 客户端连接

禁用 SSID 广播的无线客户端连接的具体操作步骤如下。

01 单击系统桌面右下角【】图标，会看到无线客户端自动扫描到区域内的所有无线信号，发现其中没有 SSID 为【ssh】的无线网络，但是会出现一个名称为【其他网络】的信号，如图 13-37 所示。



图 13-37

02 右击【其他网络】，在弹出的快捷菜单中选择【连接】选项，如图 13-38 所示。



图 13-38

03 弹出【连接到网络】对话框，在【名称】文本框中输入要连接网络的 SSID 号，本实例这里输入【ssh】，如图 13-39 所示，单击【确定】按钮。



图 13-39

04 在【安全密钥】文本框中输入无线网络的密钥，本实例这里输入密钥【sushi1986】，如图 13-40 所示，单击【确定】按钮。



图 13-40

05 单击系统桌面右下角【】图标，将鼠标放在【ssh】信号上可以看到无线网络的连接情况，如图 13-41 所示，表明无线客户端已经成功连接到无线路由器。



图 13-41

13.3 项目实施：媒体访问控制（MAC）地址过滤

网络管理的主要任务之一就是控制客户端对网络的接入和对客户端的上网行为进行控制，无线网络也不例外，通常无线 AP 利用媒体访问控制（MAC）地址过滤的方法来限制无线客户端的接入。

1. 设置无线路由器进行 MAC 地址过滤

使用无线路由器进行 MAC 地址过滤的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入“http://192.168.1.1”，如图 13-42 所示。

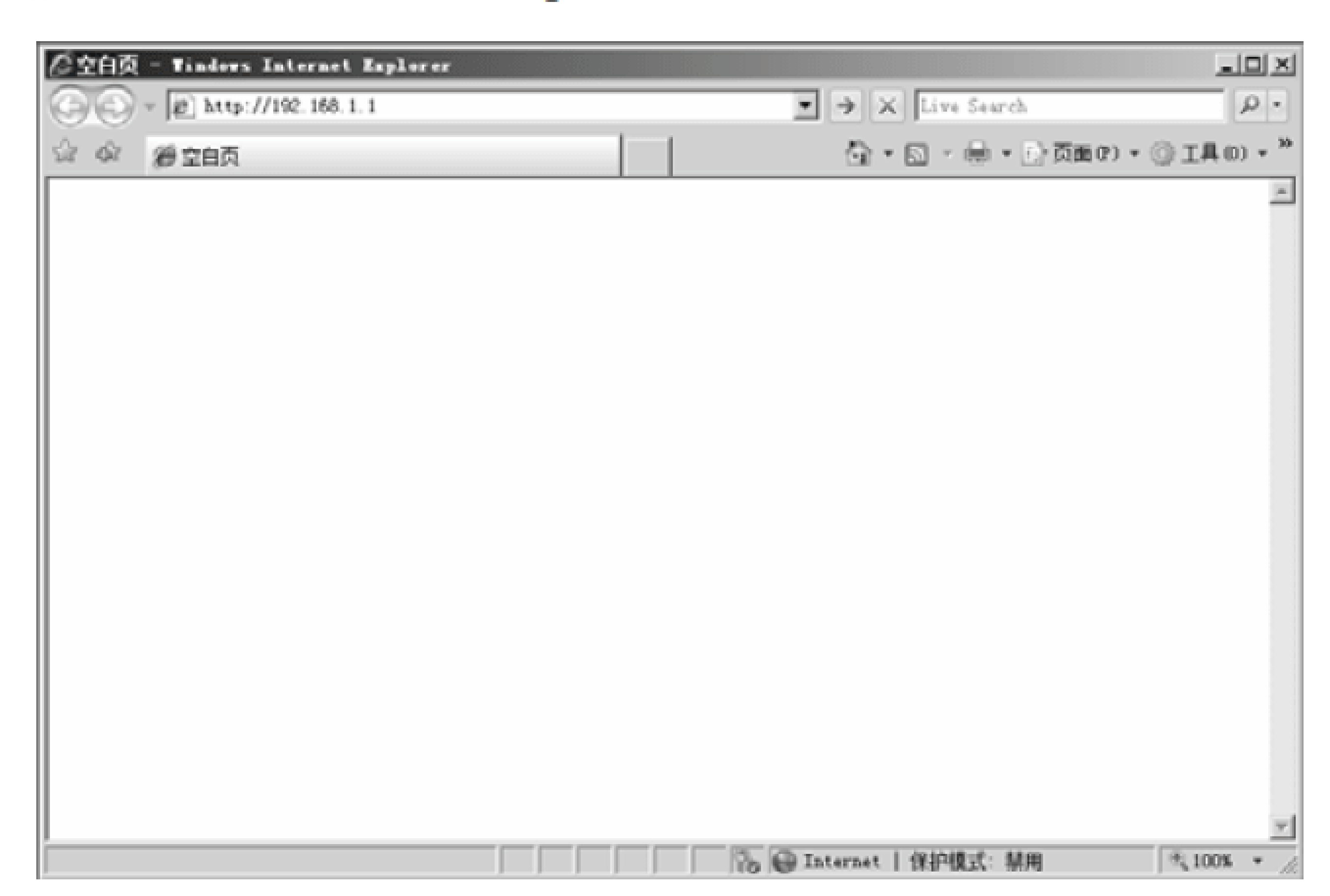


图 13-42

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为“admin”，如图 13-43 所示，单击【确定】按钮。

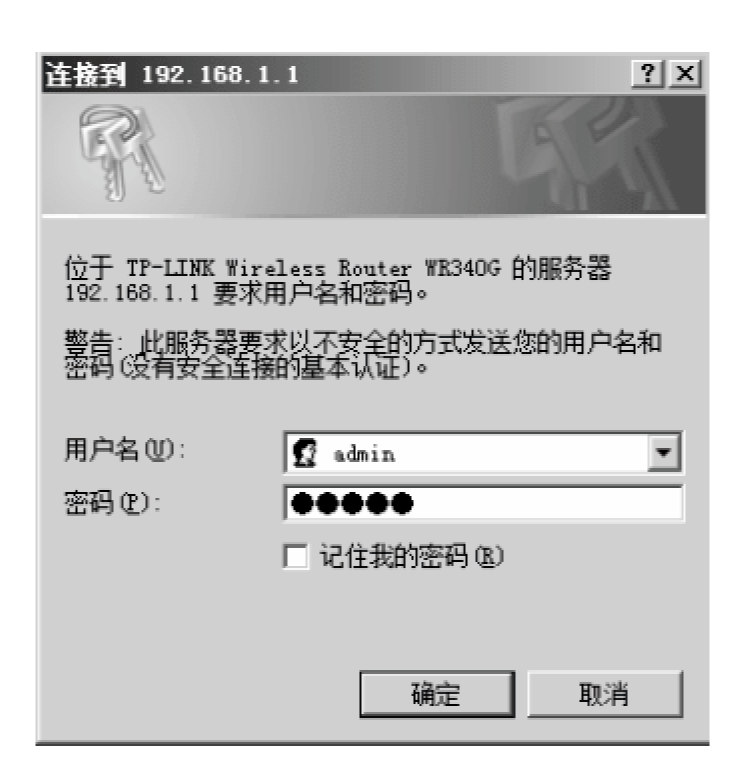


图 13-43

03 单击左侧【无线参数】➢【MAC 地址过滤】选项，默认情况 MAC 地址过滤功能是关闭状态，单击【启用过滤】按钮，开启 MAC 地址过滤功能，单击【添加新条目】按钮，如图 13-44 所示。



图 13-44

04 打开新页面，在【MAC 地址】文本框中输入无线客户端的 MAC 地址，本实例输入 MAC 地址为“00-0C-29-5A-3C-97”，在【描述】文本框中输入 MAC 描述信息“sushipc”，在【类型】下拉菜单中选择【允许】选项，在【状态】下拉菜单中选择【生效】选项，如图 13-45 所示，依照此步骤将所有合法的无线客户端的 MAC 地址加入到此 MAC 地址表后，单击【保存】按钮。



图 13-45

05 选择【过滤规则】中的【禁止】单选按钮，表明禁止在下面 MAC 列表中生效规则之外的 MAC 地址访问无线网络，如图 13-46 所示。

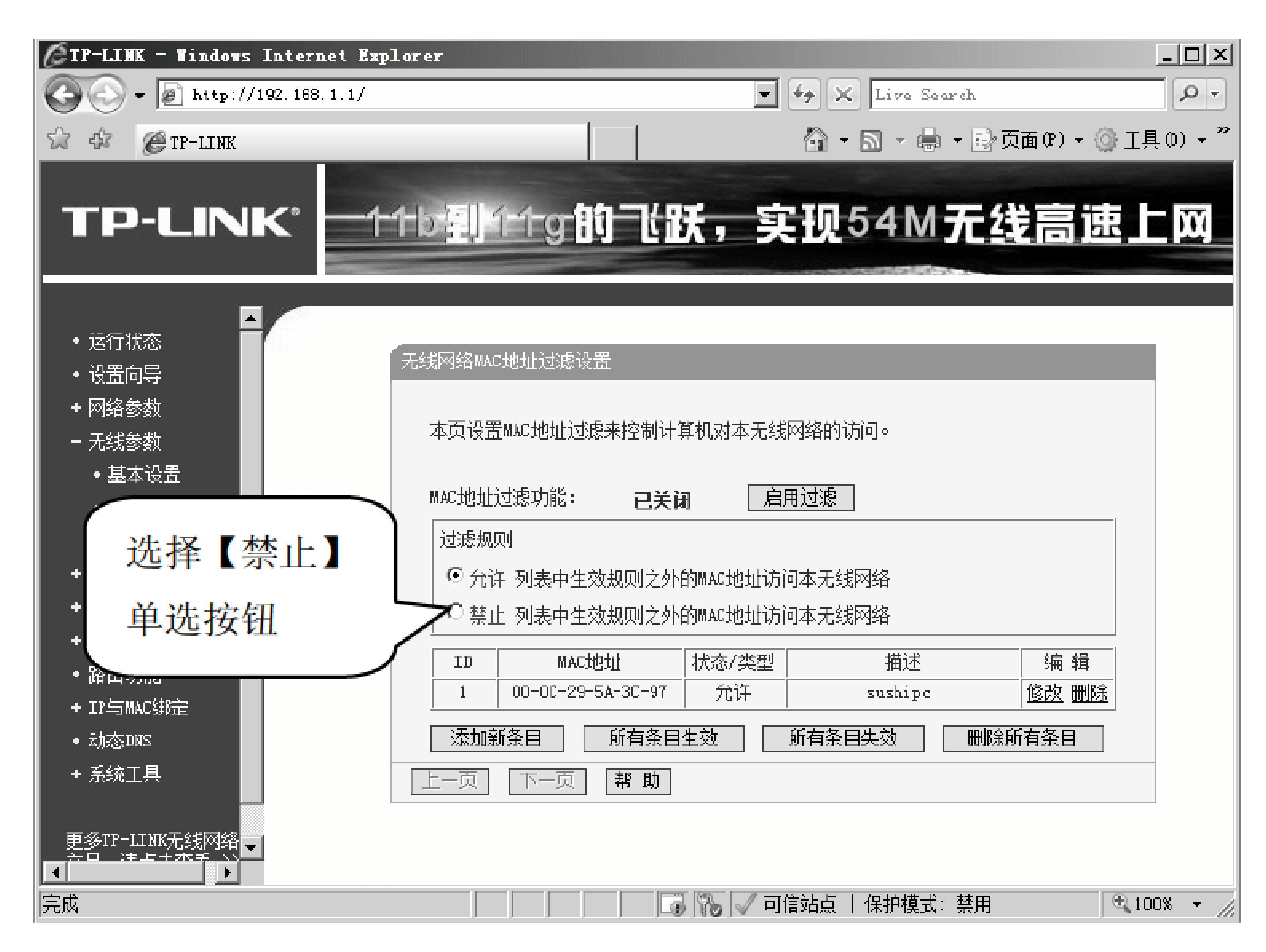


图 13-46

06 弹出【Windows Internet Explorer】提示对话框，单击【确定】按钮，更改过滤规则，如图 13-47 所示。



图 13-47

07 客户端连接，此时在无线客户端访问无线 AP 时，会发现除了 MAC 地址表中的 MAC 地址之外，其他的 MAC 地址无法再访问无线 AP，也就无法访问互联网。

13.4 专家答疑

（1）在无线路由器中对数据进行 WPA-PSK 加密设置后，无线客户端连接的时候，总是提示连接不成功，但是用无线网卡连接 WEP 加密的无线 AP 则不会出现这种问题？

答：在上面讲解的 WEP 和 WPA-PSK 加密算法，需要无线 AP 和无线客户端同时支持，由于有些老的无线客户端只支持 WEP 加密，那么这些客户端就不能使用 WPA-PSK 加密的无线 AP。

（2）将无线路由器设置完毕后，经过多次检查，无线路由器设置没有问题，但是无线客户端连接不上？

答：如果无线路由器设置没有问题，但是客户端却连接不上，主要由以下几个原因造成：

①无线 AP 的频率设置有问题，有的叫做模式。所谓无线 AP 的频率，是指无线信号传输使用的无线电频率，如果在一个区域中出现两个无线信号的频率一样，会导致数据传输失败。

②无线客户端被无线 AP 设置为访问限制，比如 MAC 地址过滤。

③无线客户端不支持无线 AP 使用的无线协议。

（3）怎么知道无线 AP 正在被哪些客户机访问？

答：查看无线 AP 已连接客户端信息的具体操作步骤如下。

01 在 IE 浏览器的地址栏中输入 “http://192.168.1.1” ，如图 13-48 所示。

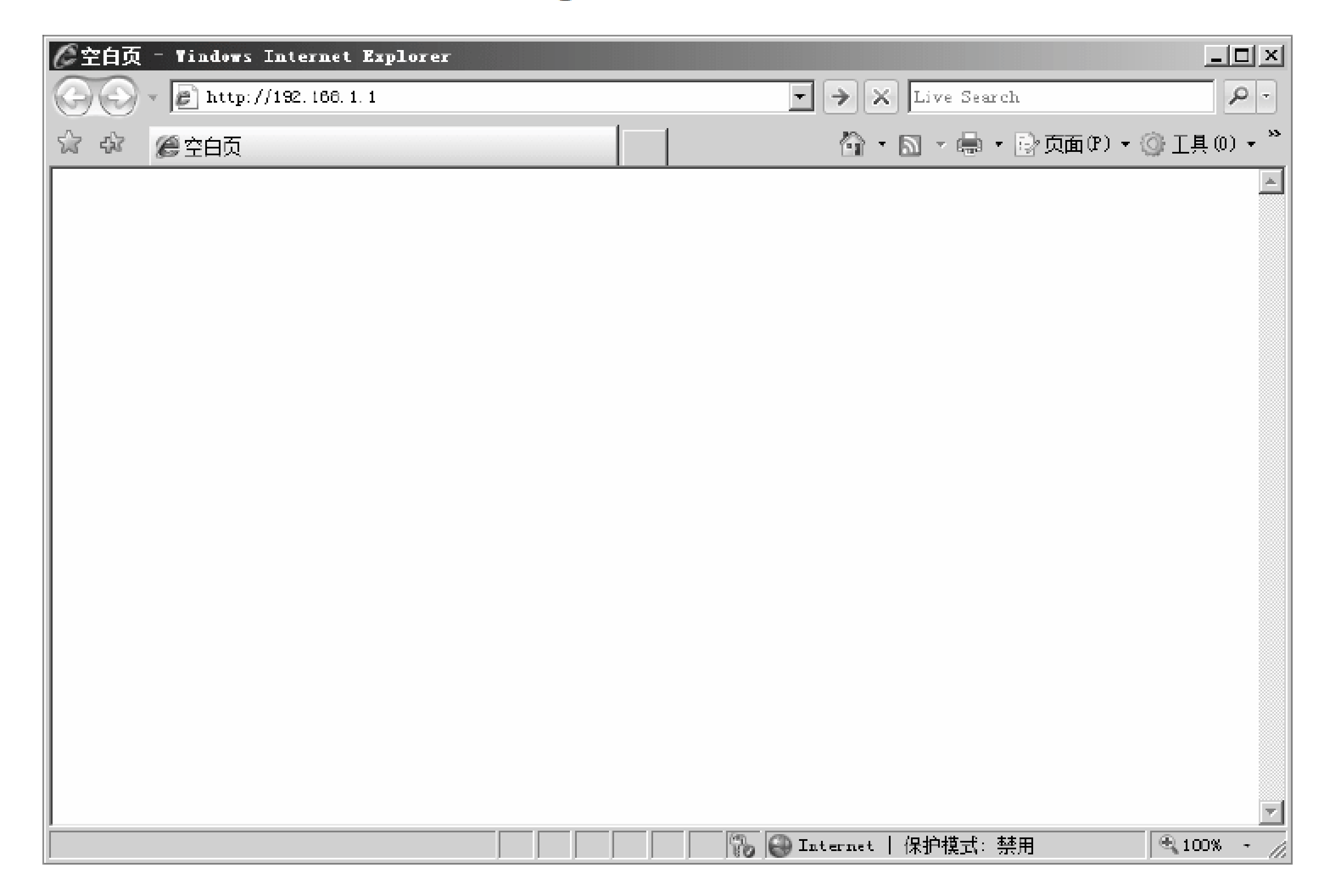


图 13-48

02 弹出【连接到 192.168.1.1】对话框，在【用户名】和【密码】文本框中分别输入用户名和密码，TP-LINK 的家用路由器的默认用户名和密码都为 “admin” ，如图 13-49 所示，单击【确定】按钮。

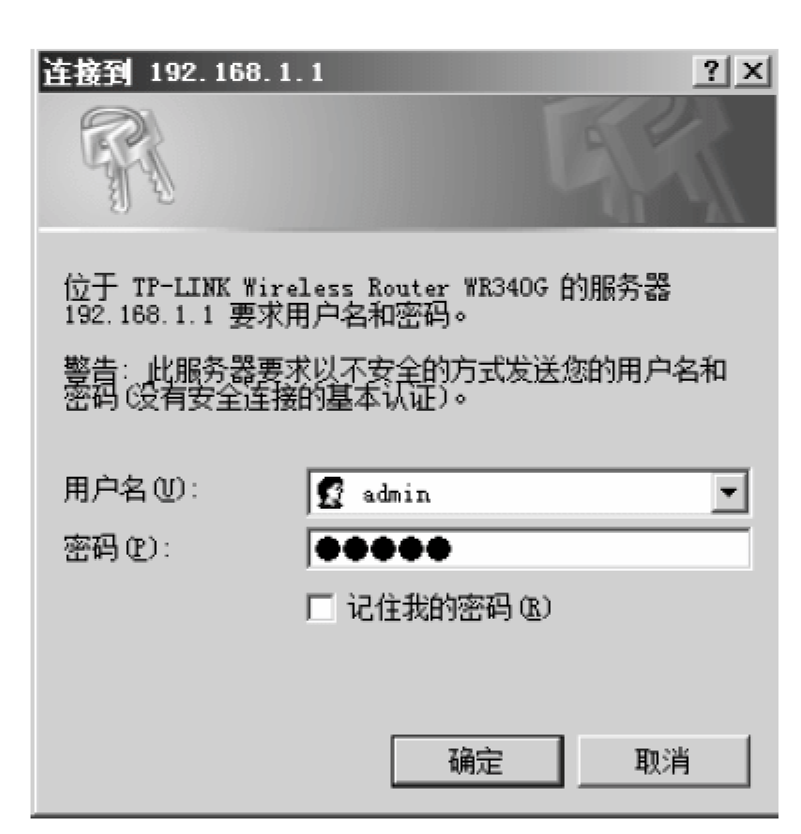


图 13-49

03 单击左侧【无线参数】➢【主机状态】选项，查看现在有哪些主机正在访问无线 AP，如图 13-50 所示。

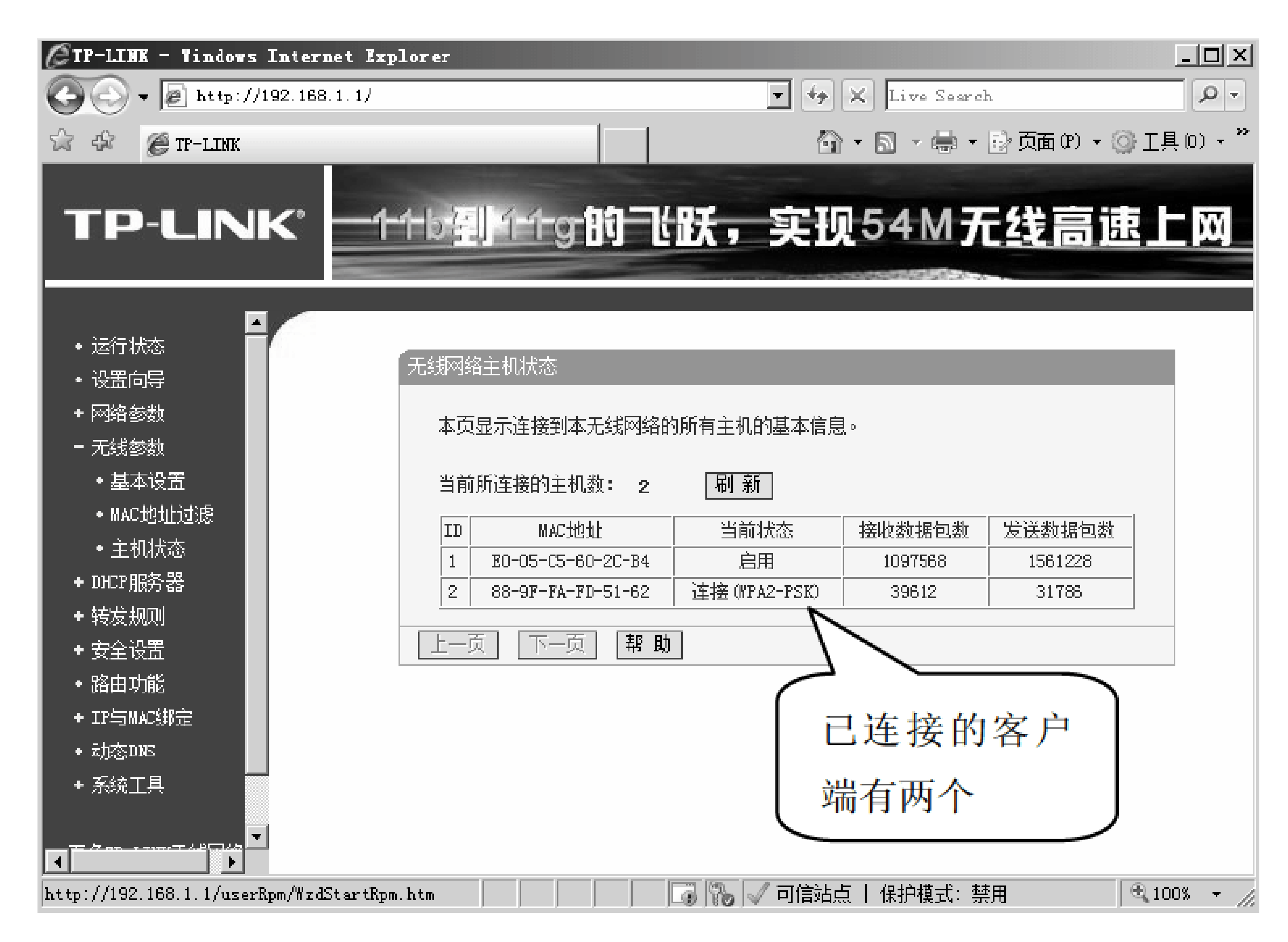

TP-LINK - Windows Internet Explorer
http://192.168.1.1/
TP-LINK
11b到11g的飞跃，实现54M无线高速上网
运行状态
设置向导
网络参数
无线参数
基本设置
MAC地址过滤
主机状态
DHCP服务器
转发规则
安全设置
路由功能
IP与MAC绑定
动态DNS
系统工具
无线网络主机状态
本页显示连接到本无线网络的所有主机的基本信息。
当前所连接的主机数： 2
刷 新
ID | MAC地址 | 当前状态 | 接收数据包数 | 发送数据包数
1 | E0-05-C5-6C-2C-B4 | 启用 | 1097568 | 1561228
2 | 88-9F-FA-FD-51-62 | 连接 (WPA2-PSK) | 39612 | 31786
上一页
下一页
帮 助
已连接的客户端有两个
http://192.168.1.1/userRpm/WzdStartRpm.htm
可信站点 | 保护模式：禁用
100%

图 13-50

第 14 章　企业防火墙

随着依赖网络、计算机办公的人和企业越来越多，相应的网络威胁也层出不穷，如常见的病毒、木马、网络攻击等等。一旦企业网络或家庭个人计算机遭受网络威胁，都会带来巨大的损失，尤其是企业网络。目前解决外网攻击最有力的手段就是防火墙技术。

14.1　防火墙概述

提起防火墙技术，大多数人都接触过，平时使用 Windows 系统时，为了个人主机安全通常会开启 Windows 自带的防火墙，以保护个人主机的安全。另外，局域网内往往会出现 ARP 病毒或攻击，使个人主机遭受地址欺骗，这时可以使用 ARP 防火墙阻止外部地址欺骗的攻击流，保护主机安全。但在复杂的企业网络环境中，网络攻击的数量、威胁都很大，一个单机防火墙根本解决不了全网的网络威胁，这时就需要使用企业防火墙。

14.1.1　什么是企业防火墙

企业防火墙是指由软件和硬件设备构成的用于限制企业内网和外网之间流量访问的安全架构。防火墙是一种访问控制和隔离技术，是网络安全区域和不安全区域的屏障。

企业防火墙可以作为内网的安全网关，确保内网免受外网非法用户的入侵。防火墙可以通过服务访问规则、验证技术、包过滤和应用网关四部分功能，使流入流出的所有信息被检测被控制，所有具有安全隐患的流量都可以被拒绝转发。

在企业网内部有很多用户，并不是每一个用户都能安全的使用计算机。大多数用户对计算机的安全配置了解甚少，经常出现不安装防火墙、杀毒软件，处于“裸奔”状态的主机，再加上有些用户上网行为不规范，很容易成为外网网络攻击者实施全网攻击的跳板。与其逐个的去督促管理用户安全使用计算机，不如在网络出口架设一套防火墙系统显得更为有效。

企业防火墙并不是在网络出口位置进行安装了就能起到保护全网的作用，在架设防火墙系统时还应当设计一套安全、可靠的访问控制规则，准确的拒绝、过滤具有安全隐患的流量，而让合法流量顺利通过。所以，一套完整的企业防火墙系统应当由两部分组成：软硬件防火墙环境和防火墙配置策略。

14.1.2 防火墙的分类

防火墙技术自出现起，发展至今已经产生了很多的类型。从功能、技术、结构、性能等多个方面可以对防火墙进行分类，如表 14-1 所示。

表 14-1

分类方式	类别		
软硬件构成形式	软件防火墙	硬件防火墙	芯片级防火墙
防火墙功能技术	包过滤防火墙	状态检测防火墙	应用代理型防火墙
防火墙结构	单一主机防火墙	集成路由防火墙	分布式防火墙
防火墙的应用部署位置	边界防火墙	个人防火墙	混合防火墙
防火墙性能	百兆级防火墙	千兆级防火墙	
防火墙使用方法	网络层防火墙	物理层防火墙	链路层防火墙

防火墙的种类繁多，选择时考虑最多的还是它的功能技术。下面介绍一下包过滤防火墙、状态检测防火墙和应用代理型防火墙。

1. 包过滤防火墙

包过滤防火墙将对每一个接收到的包进行分析，通过匹配过滤规则，做出允许或拒绝的决定。过滤规则匹配的主要是 IP 数据报的报头信息，包括：源 IP 地址、目的 IP 地址、协议类型（TCP 包、UDP 包、ICMP 包）、源端口、目的端口等报头信息。当数据包通过防火墙时，会逐个检测每一条规则，一旦有信息匹配成功，就会按照过滤规则进行转发，或者丢弃。如果没有规则和数据包匹配，防火墙会采用默认规则，一般默认丢弃所有不匹配数据包。

包过滤防火墙需要处理数据包的 IP 信息和 TCP/UDP 信息来匹配规则，所以它工作在网络层和传输层。和代理服务器相比，它只需要将数据包拆到第四层，处理速度要快一些。对于网络攻击单一，威胁一般的中小网络比较适用。而对基于应用层的威胁不能做出反应，所以在安全级别较高的网络中不建议选择。

同时，包过滤防火墙在价格上一般比代理防火墙便宜，也适合中小企业使用。

当然，包过滤防火墙也存在一些问题。首先，它只能过滤到端口，却无法分析数据内容，利用安全端口隐藏攻击的数据包无法过滤。其次，网络环境比较复杂的情况下，网络管理员需要配置的访问规则将会很复杂，不利于管理。

2. 状态检测防火墙

状态检测防火墙是传统包过滤防火墙的功能扩展，除了有包过滤功能外，还可以抽取数据包和应用层状态相关的信息，并以此为依据决定是否允许数据包通过。能够实现该功能主要是依靠状态检测防火墙内部的一个不需要配置、自动产生的状态表。状态表规定了允许的源 IP 地址和目的 IP 地址、源端口和目的端口、数据包的 TCP 序列号和标志位等信息。

状态检测防火墙除了拥有包过滤防火墙的优点外，它对应用也是透明的，且在安全性上做了较大幅度的提升。防火墙接收到数据包后，首先会逐个检测过滤策略，如果没有策略允许通过，该数据包被丢弃，如果有允许策略匹配，数据包将被接受，并建立连接状态，后续数据包以此连接状态为标准进行匹配，一致则被转发，不一致被丢弃。

整体来看，状态检测防火墙具有安全性高、性能好、扩展性好、配置方便等优点，所以这类防火墙应用比较广泛。但是状态检测防火墙和包过滤防火墙一样，依然只是检测数据包的网络层和传输层信息，不能分析更高层次的数据，对于隐藏在应用层的攻击无法进行阻止。

3. 应用代理型防火墙

应用代理型防火墙也叫应用层网关防火墙。这种防火墙通过在 TCP 连接中加入一种 Proxy（代理）技术的方式实现安全隔离。从网络内部发出的数据包，在经过防火墙后，会被处理成以防火墙外部网卡为源的数据包，这样可以达到隐藏内网环境的作用。

应用代理型防火墙在实现代理转发的过程中，会对数据包的应用层数据作出分析，安全级别远远高于前两种防火墙。到目前为止，这类防火墙也是公认的最安全的防火墙。

14.1.3 防火墙联网模型

有了防火墙之后，又当如何连接呢？这是在防火墙部署过程中最重要的设计内容。直接影响到整个网络的应用和安全性。下面详细介绍 4 种常用的防火墙联网模型。

1. 双向边缘防火墙联网模型

这类防火墙联网模型比较简单，只要防火墙具备两个接口就可以实现，通常适用于中小企业，如图 14-1 所示。

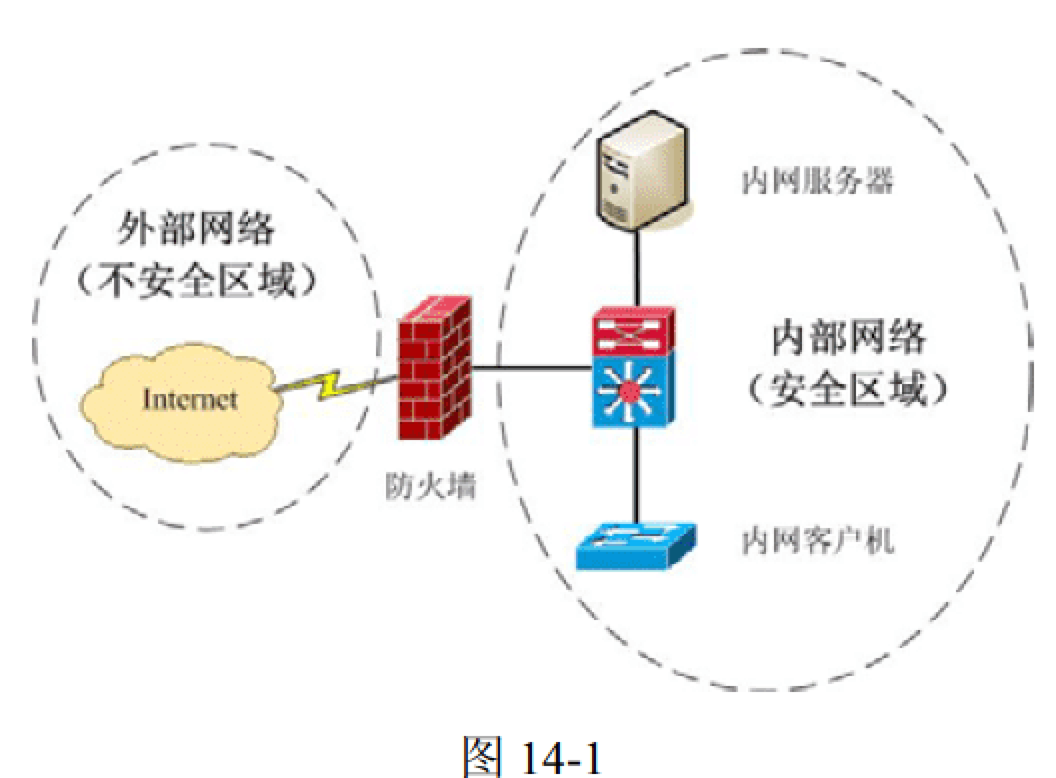


图 14-1

2. 带有 DMZ 区的 3 向防火墙联网模型

这类防火墙联网模型在双向边缘防火墙基础上增加了一个独立的 DMZ（隔离区），该区域用于放置对外网公开发布的服务器，如企业 WEB 服务器、邮件服务器等。DMZ 区的意义在于，当外部网络访问企业网站时，只能访问到 DMZ 区，而不能访问内部网络，相当于一个外部不安全区域和内部安全区域的缓冲区，相比把服务器和内网客户机放置在同一区域安全了很多。通过这样一个 DMZ 区域，更加有效地保护了内部网络的安全。

部署这类防火墙联网模型比较复杂，防火墙本身必须支持 DMZ 区功能并且有可用的 DMZ 接口，如果是软件防火墙，系统平台至少也要有三个网卡接口，如图 14-2 所示。

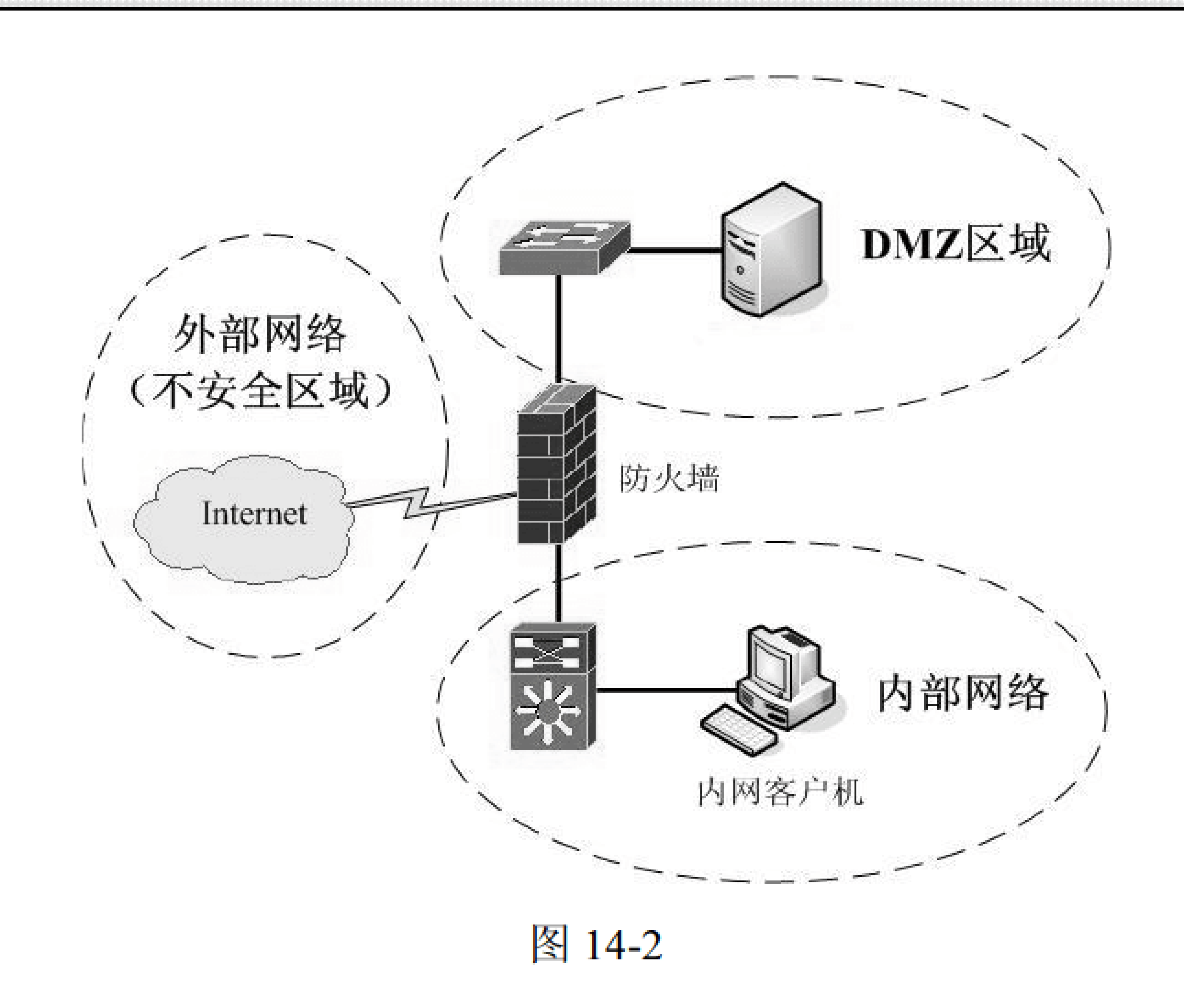


图 14-2

3. 前后端防火墙联网模型

前后端防火墙联网模型和带有 DMZ 区的 3 向防火墙联网模型比起来略有些复杂，将 DMZ 区独立于两个防火墙之间，如图 14-3 所示。这样部署会使内部安全网络和外部的不安全网络实现物理隔离，更好的保证内外网通信安全。

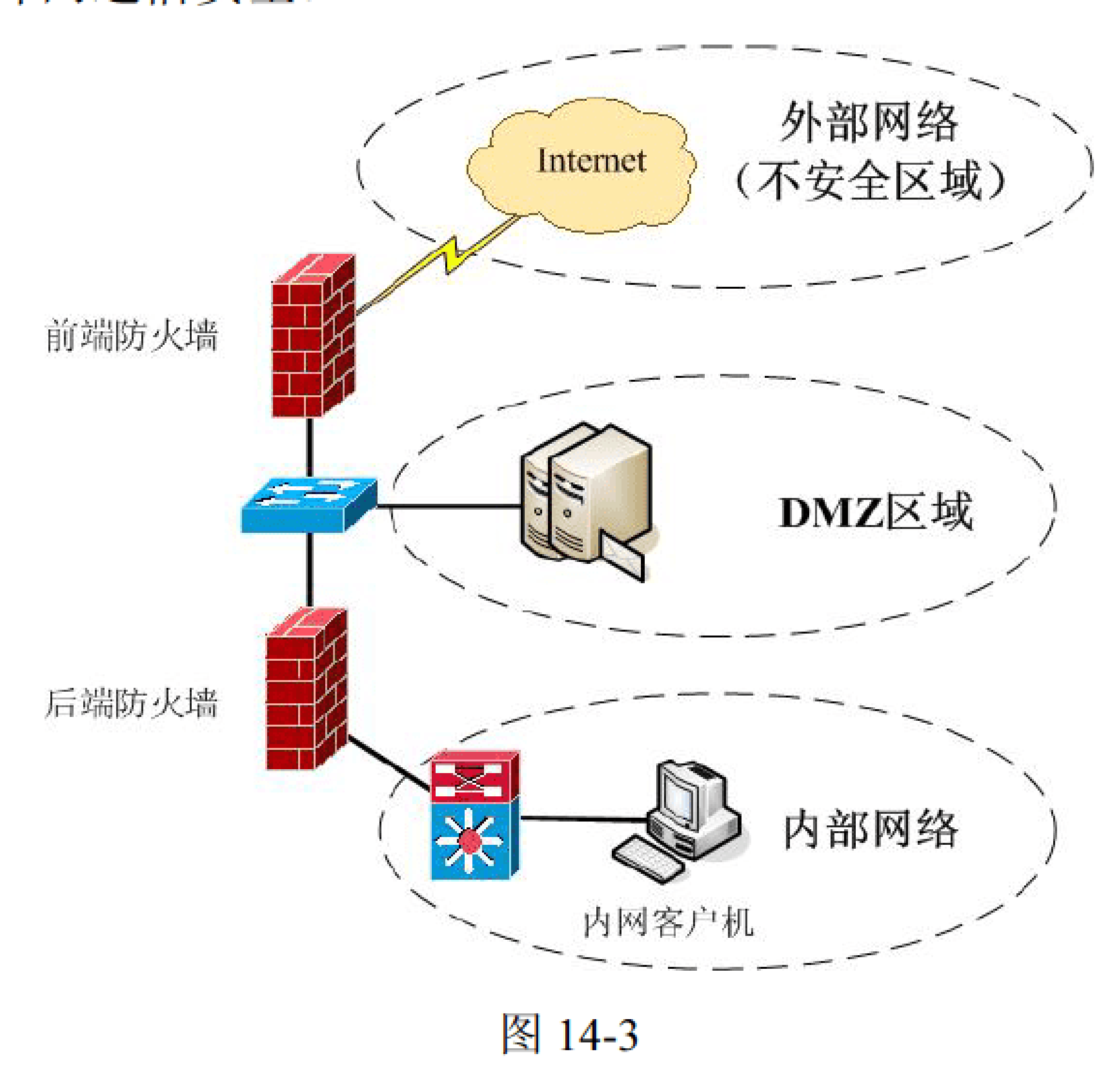


图 14-3

4. 高可用的防火墙联网模型

高可用的防火墙联网模型，由两个防火墙同时进行隔离、过滤、转发工作。通信工作由两个防火墙分担进行，提高了工作效率。如果有一个防火墙出现了故障，另一个防火墙依然可以正常工作，提高了网络的可用性。这类防火墙联网模型一般适用于对性能和可用性要求比较高的大中型网络，以及一些特殊的中小型网络。

这类防火墙联网模型部署起来相对比较复杂，不但在配置上比较复杂，对设备的硬件要求也比较高，特别是接口数量，需要有足够的接口做冗余连接，如图 14-4 所示。

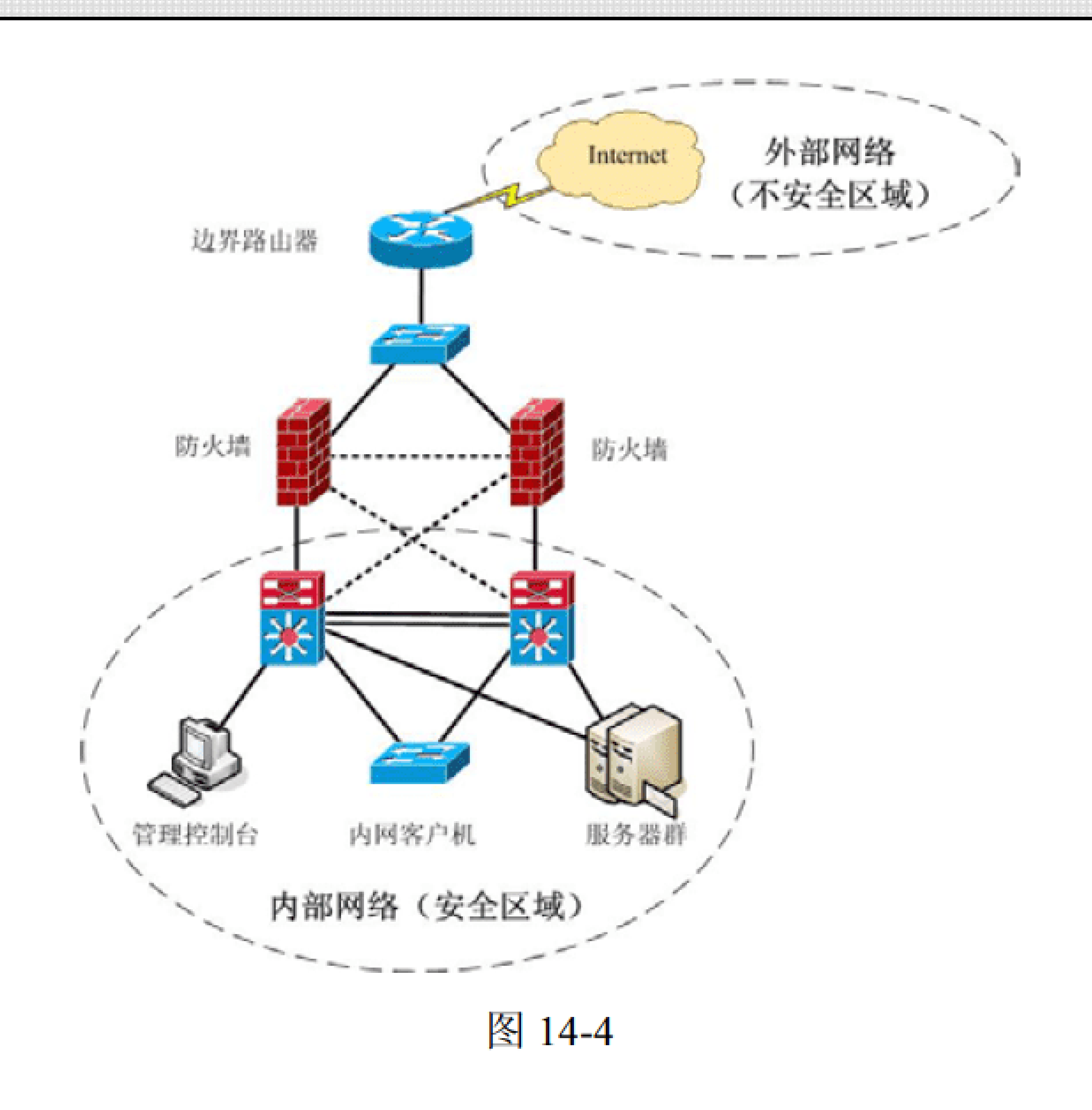


图 14-4

14.1.4 产品选型

企业防火墙在网络环境的安全管理系统中分量很重，一般的企业在设计网络安全方案时，首先考虑的就是增加防火墙。但是不同的企业，选择防火墙时有所差异。防火墙并不是越高端就越好，需要结合网络的自身情况，需要考虑的因素有以下几点。

1. 类型

防火墙有很多分类，有硬件防火墙、软件防火墙、代理防火墙、包过滤防火墙等多种类别，首先要选择的就是类型。一般中小企业使用最多的是包过滤和状态检测防火墙，代理防火墙在安全性要求较高的大型网络中使用比较多。

2. 性能

不同的产品其性能差异很大，一般硬件防火墙比软件防火墙在稳定性上要好很多，因为硬件防火墙不会受系统漏洞的影响。同时，选择时应注意大厂商的产品稳定性比小牌企业好很多。

除此之外，还要比较其性能能参数是否符合企业需求，主要性能指标有：过滤方式、地址绑定、访问控制、代理服务、带宽支持、地址转换、日志功能、路由功能、认证功能、邮件认证等。

3. 联网模型

根据企业业务需求，可能会实施不同的联网模型，但并不是所有防火墙都可以支持各类联网模型的使用，如果要架设双核心、高可用性防火墙模型的话，防火墙的网络接口数量要求有很多，又比如需要架设带 DMZ 区的三向防火墙，就必须要能够支持 DMZ 功能的。

4. 网络管理水平

选择防火墙时还需要考虑当前网络管理员的管理能力，并不是品牌好、性能好、服务好就能起到作用，还需要网络管理员使用好。有些防火墙配置起来需要较高的技术水平，比如 Cisco 的

ASA 防火墙，如果不了解其应用原理和配置命令，操作起来很难。而像 ISA Server 2006 软件防火墙，虽然也比较高端，但是其 Windows 下的全中文窗口配置界面环境使得管理员很容易操作。

5. 价格

有些企业在选择防火墙时考虑价格因素比较多，虽然碍于企业经济实力不得不考虑，但是最好将其放到最后一位。如果一个企业虽小，但是其所有业务都和服务器的应用程序和数据库有关，一味的顾虑价格，很可能降低数据的安全性保障。

通常使用比较多的防火墙有 ISA Server 2006、Cisco ASA、天融信、H3C、飞塔、启明星辰等。如果使用软件防火墙，可以使用 ISA Server 2006；如果使用硬件防火墙，则可以考虑国产的几款产品。

14.2 项目实施 1：架设 ISA 企业防火墙

ISA Server 2006 是微软公司的一款防火墙产品，很多中小企业都在使用，下面详细介绍 ISA 企业防火墙的环境搭建与配置。

14.2.1 模拟企业网络搭建实验环境

ISA 企业防火墙是安装在 Windows 系统内的软件防火墙，下面在 Windows Server 2003 环境下搭建其模拟实验环境。

1. ISA 企业防火墙安装配置要求

ISA 防火墙处于网络的关键位置，需要保证其运行环境的稳定性，所以服务器需要满足一定的配置要求，详细要求如表 14-2 所示。

表 14-2

组件	配置要求
操作系统	Windows server 2003 32 位操作系统
处理器	装有 733MHz Pentium III 或更高的处理器
硬盘	至少 150MB 可用空间，分区为 NTFS 格式分区；运行时需要更多额外空间保存 Web 高速缓存等内容
内存	至少 512MB，建议使用更大容量
其他	网络适配器根据联网模型进行配备，键盘、显示器、鼠标、光驱等普通配置即可


提 示

以上配置要求只是最低性能标准，如果网络通信业务量比较大，建议使用更高的系统配置。

2. ISA 企业防火墙环境部署

在介绍 ISA 企业防火墙的配置内容时，以图 14-5 联网方式进行讲解。主要由四台虚拟机进行

模拟实验。

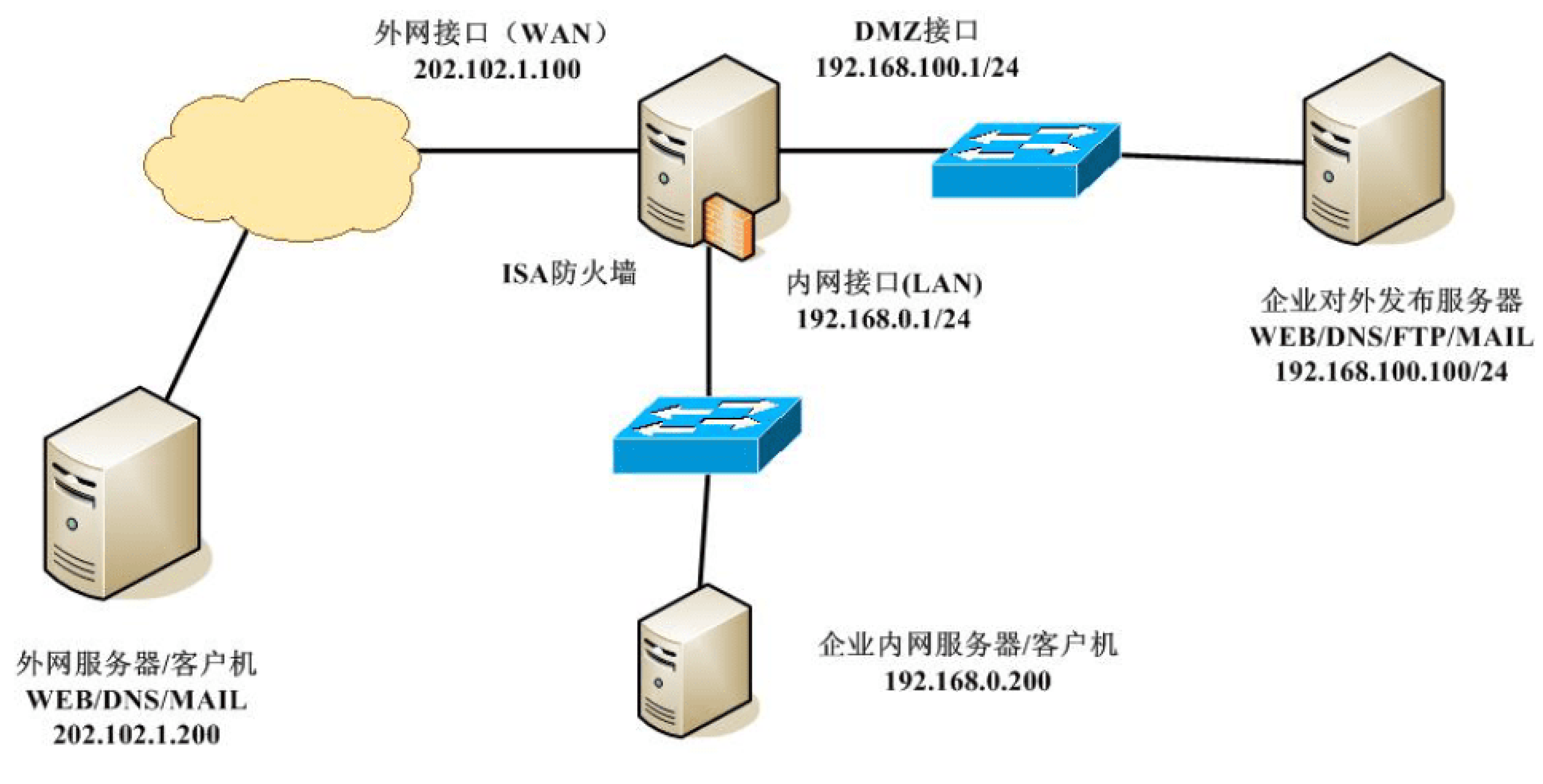


图 14-5



提 示

本实例只做 ISA 企业防火墙的配合，内网、外网、DMZ 区的服务器和客户机不做配置讲解。

14.2.2 安装 ISA 2006 防火墙

在使用 ISA 2006 防火墙之前，需要先安装其应用程序，具体的操作步骤如下。

01 将 ISA 2006 安装光盘放入光驱内，系统读取光盘内容，弹出【Microsoft ISA Server 2006 安装程序】对话框，单击【安装 ISA Server 2006】选项，如图 14-6 所示。

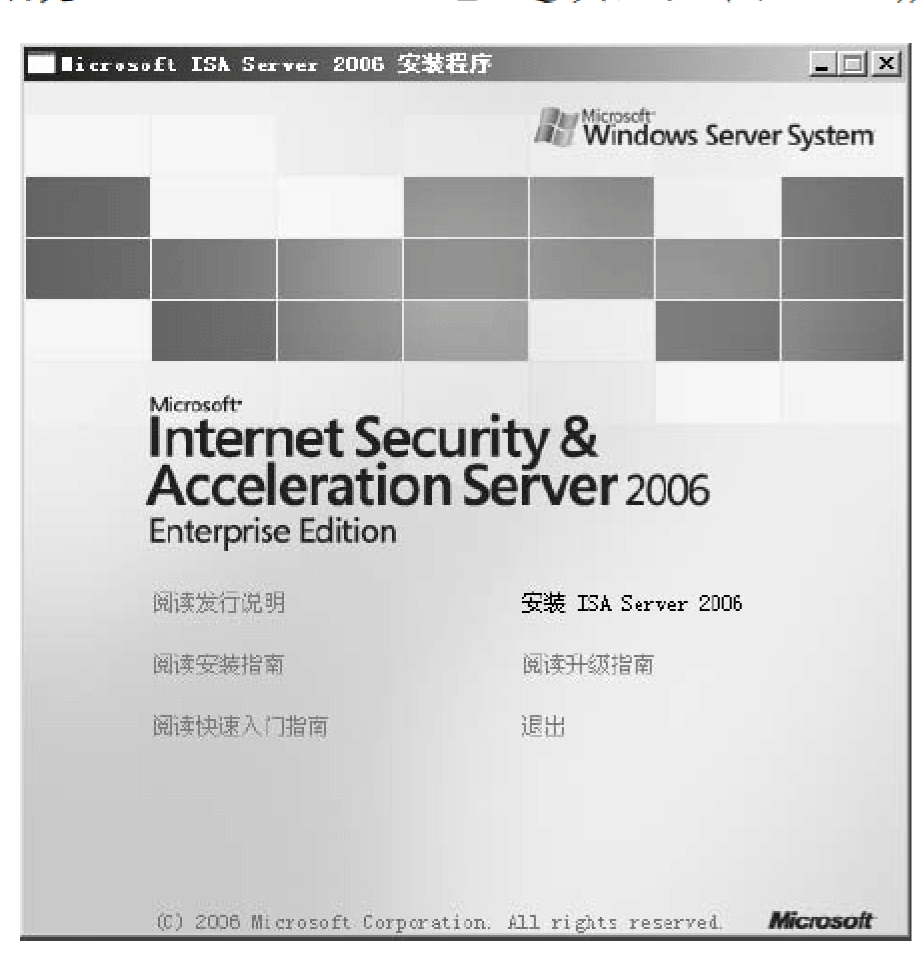


图 14-6

02 弹出【欢迎使用 Microsoft ISA Server 2006 的安装向导】对话框，如图 14-7 所示，单击【下一步】按钮。

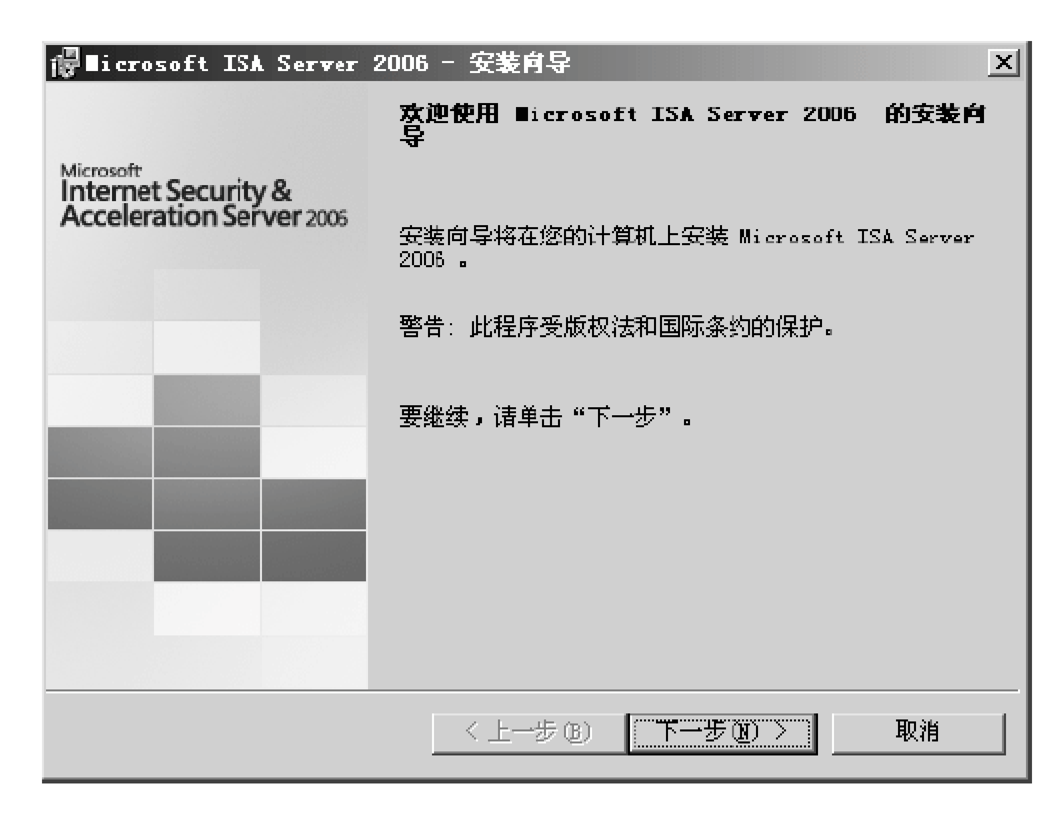


图 14-7

03 弹出【许可协议】对话框，选择【我接受许可协议中的条款】单选按钮，如图 14-8 所示，单击【下一步】按钮。



图 14-8

04 弹出【客户信息】对话框，在其中输入匹配信息及产品序列号，如图 14-9 所示，单击【下一步】按钮。

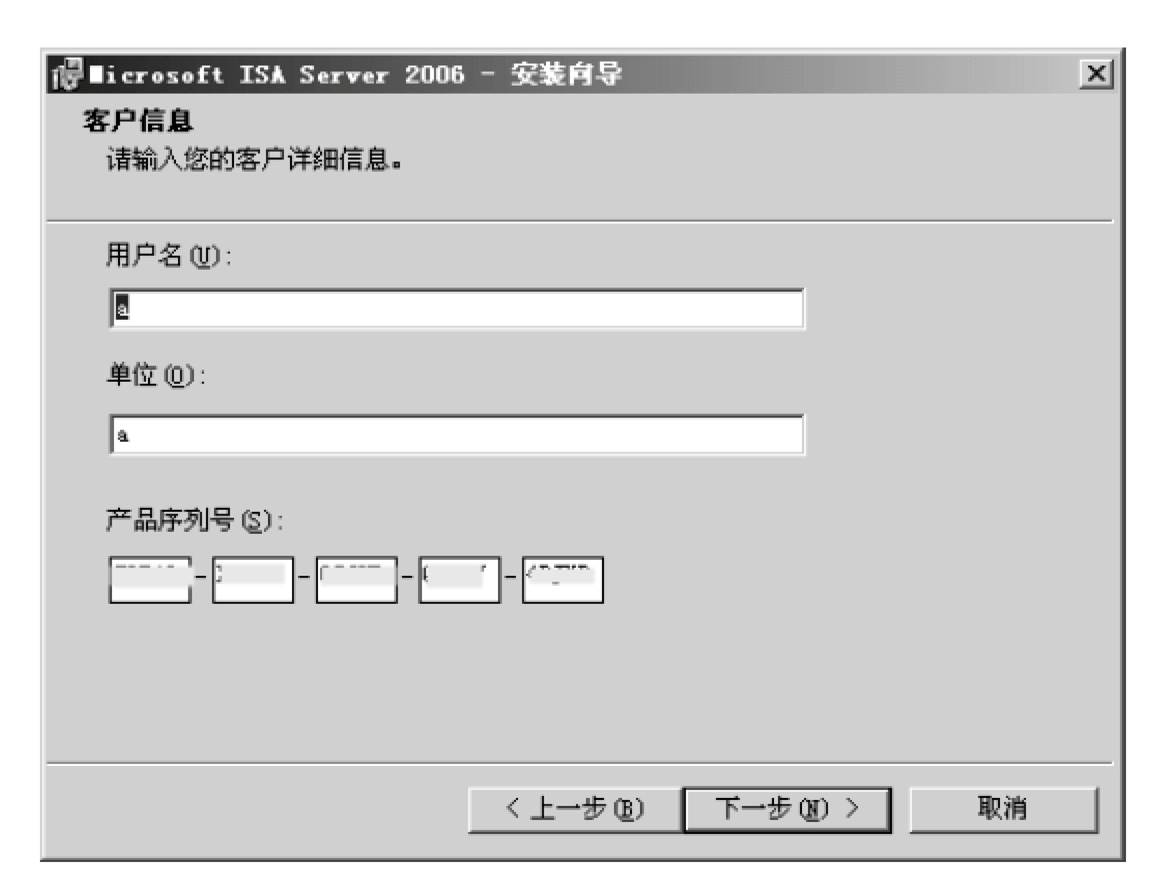


图 14-9

05 弹出【安装方案】对话框，选择【同时安装 ISA Server 服务和配置存储服务器】单选按钮，如图 14-10 所示，单击【下一步】按钮。

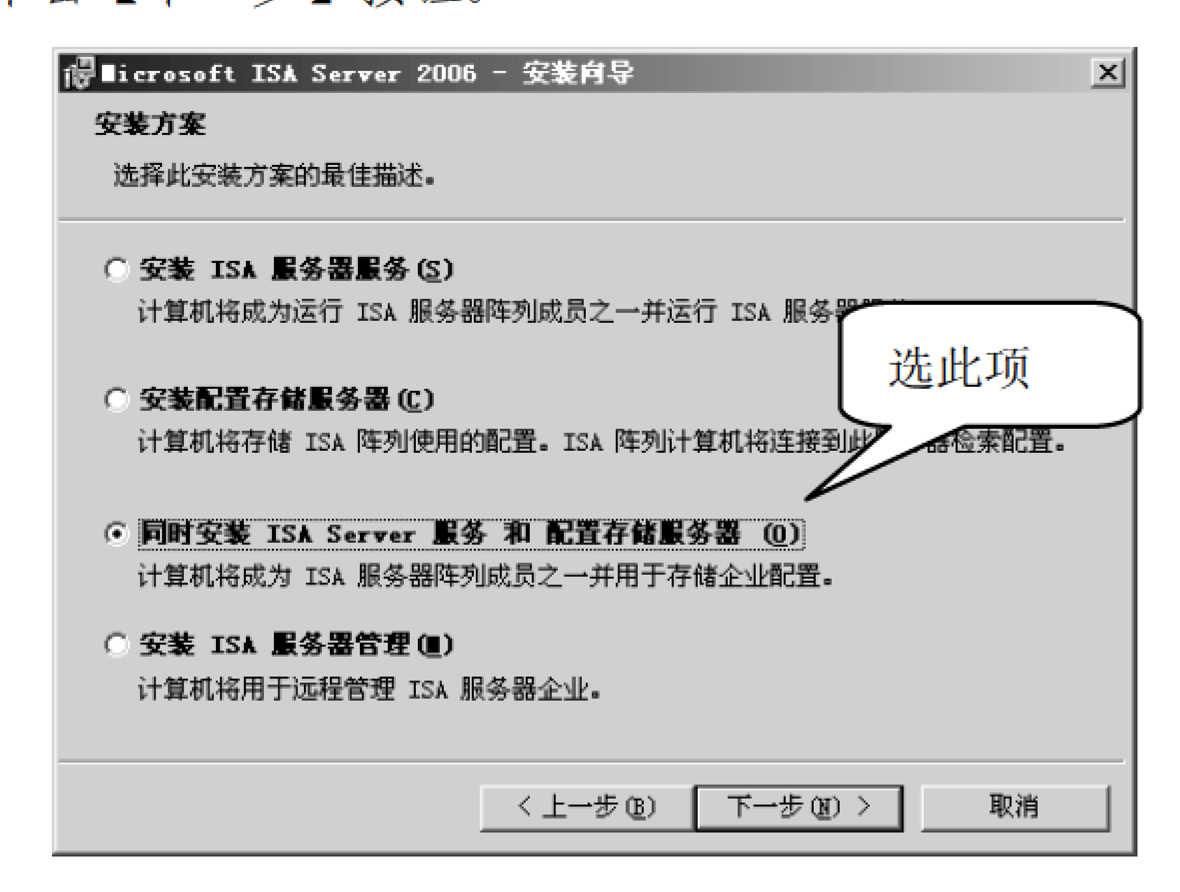


图 14-10

06 弹出【组件选择】对话框，默认选择安装所有组件，单击【更改】按钮，如图 14-11 所示，可以改变程序的安装目录位置，本实例采用默认配置，单击【下一步】按钮。

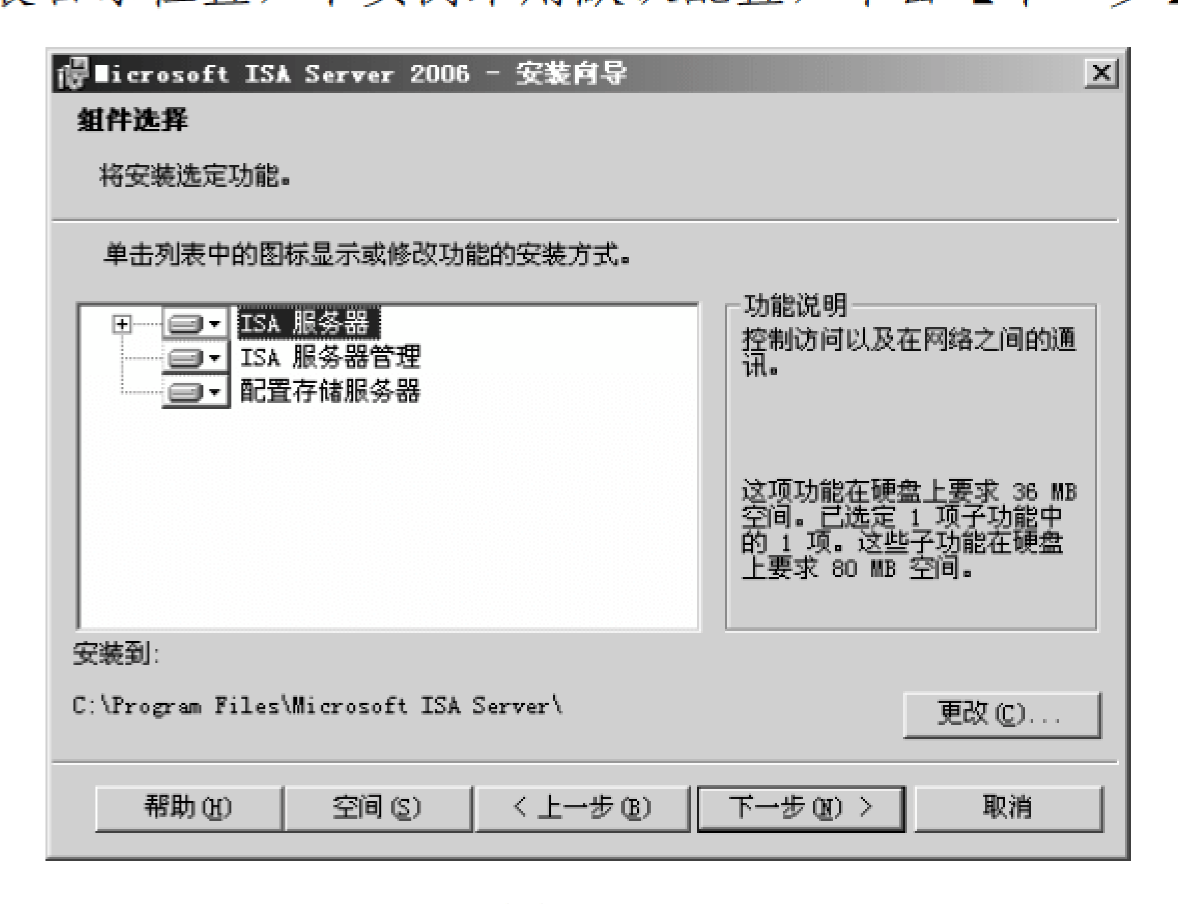


图 14-11

07 弹出【企业安装选项】对话框，由于初次搭建 ISA 防火墙，所以选择【创建新 ISA 服务器企业】单选按钮，单击【下一步】按钮，如图 14-12 所示。

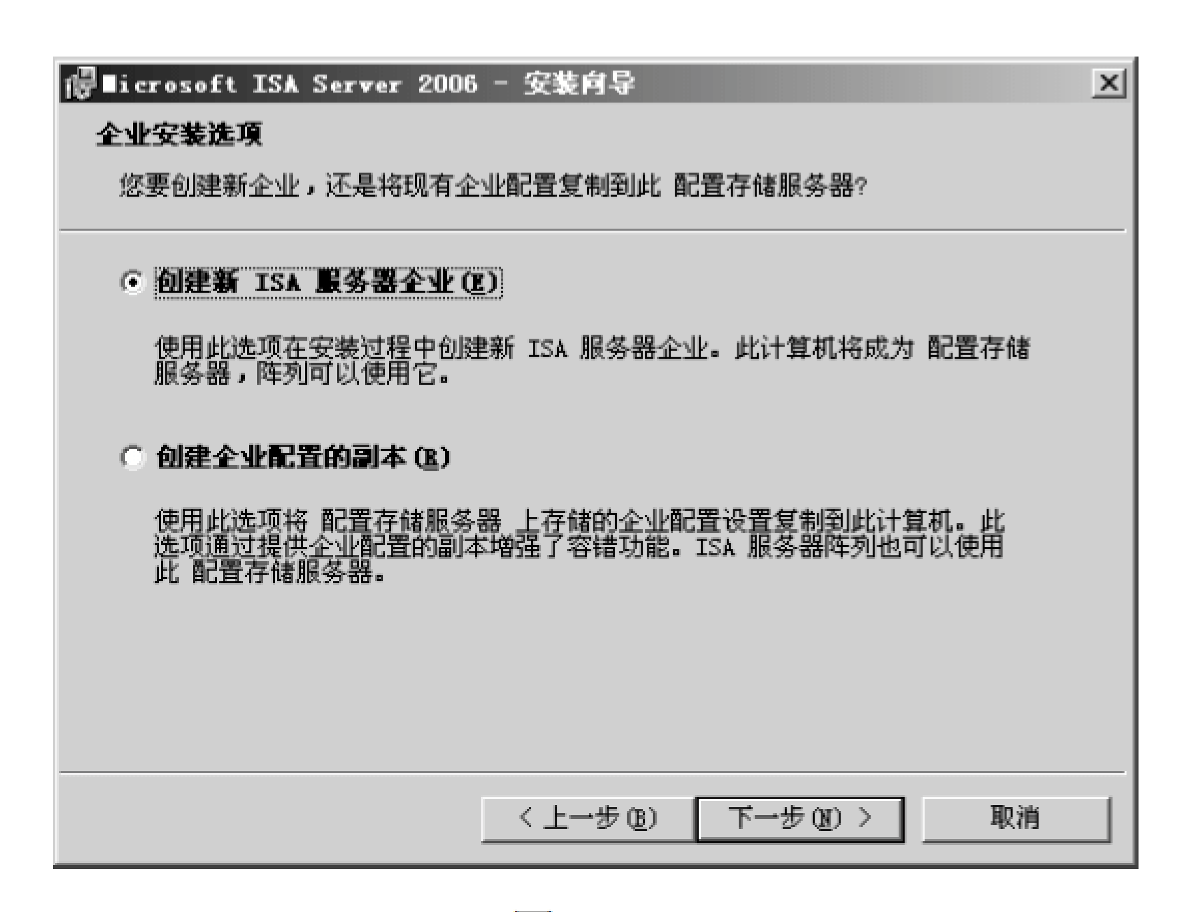


图 14-12

08 弹出【新建企业警告】对话框，如图 14-13 所示，单击【下一步】按钮。

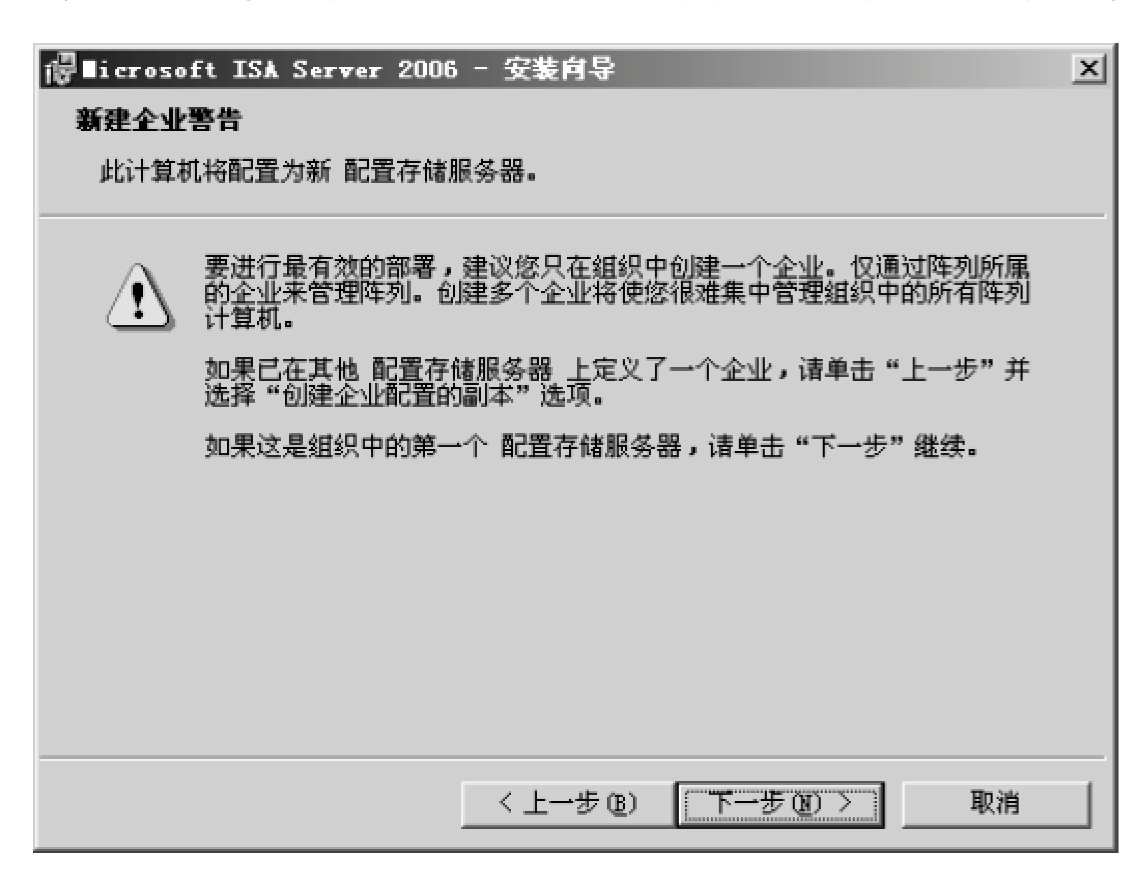


图 14-13

09 弹出【内部网络】对话框，单击【添加】按钮，如图 14-14 所示，指定 ISA 内部网络的地址范围。

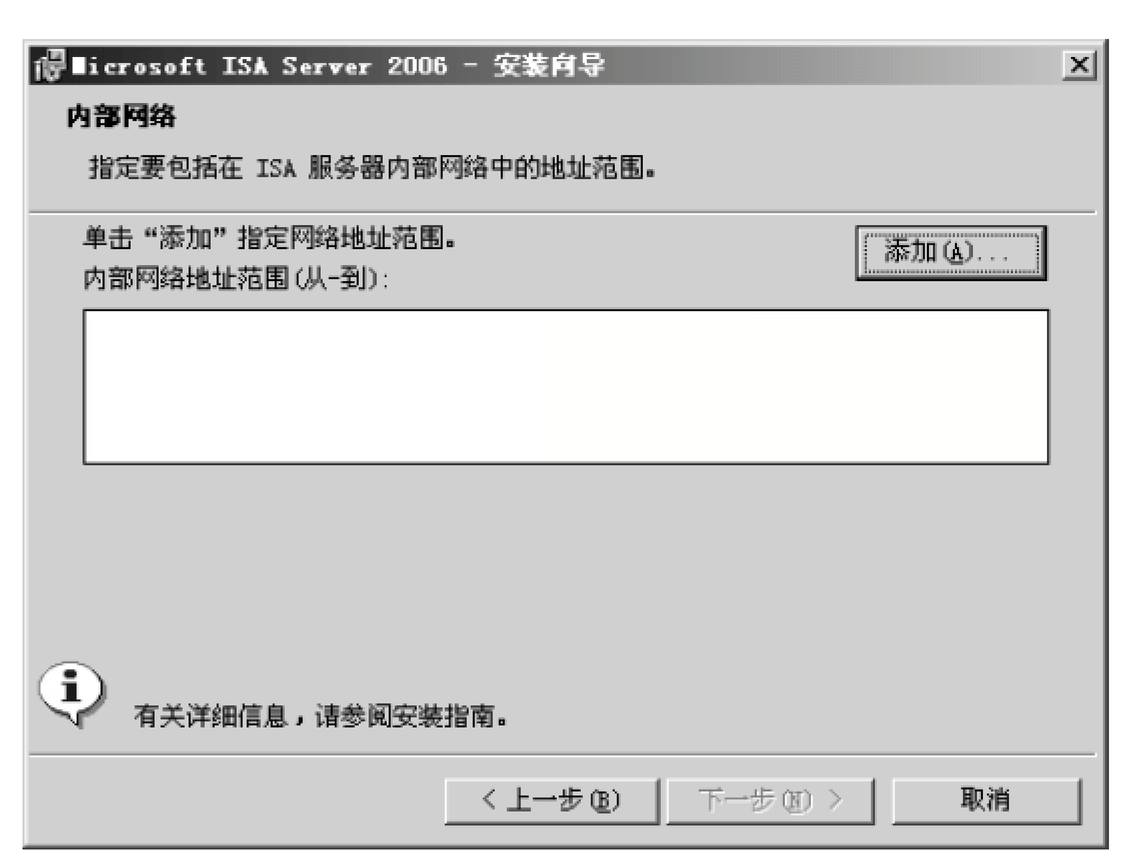


图 14-14

10 弹出【地址】对话框，可以单击【添加适配器】按钮指定内部网卡，也可以单击【添加

范围】按钮指定内部网络地址范围，本实例选择指定内部网卡，如图 14-15 所示。



图 14-15

11 弹出【选择网络适配器】对话框，在【网络适配器】窗格中显示了服务器的三块网卡，选择【LAN】复选框，在【网络适配器详细信息】窗格中显示出 LAN 网卡的详细信息，如图 14-16 所示，单击【确定】按钮。

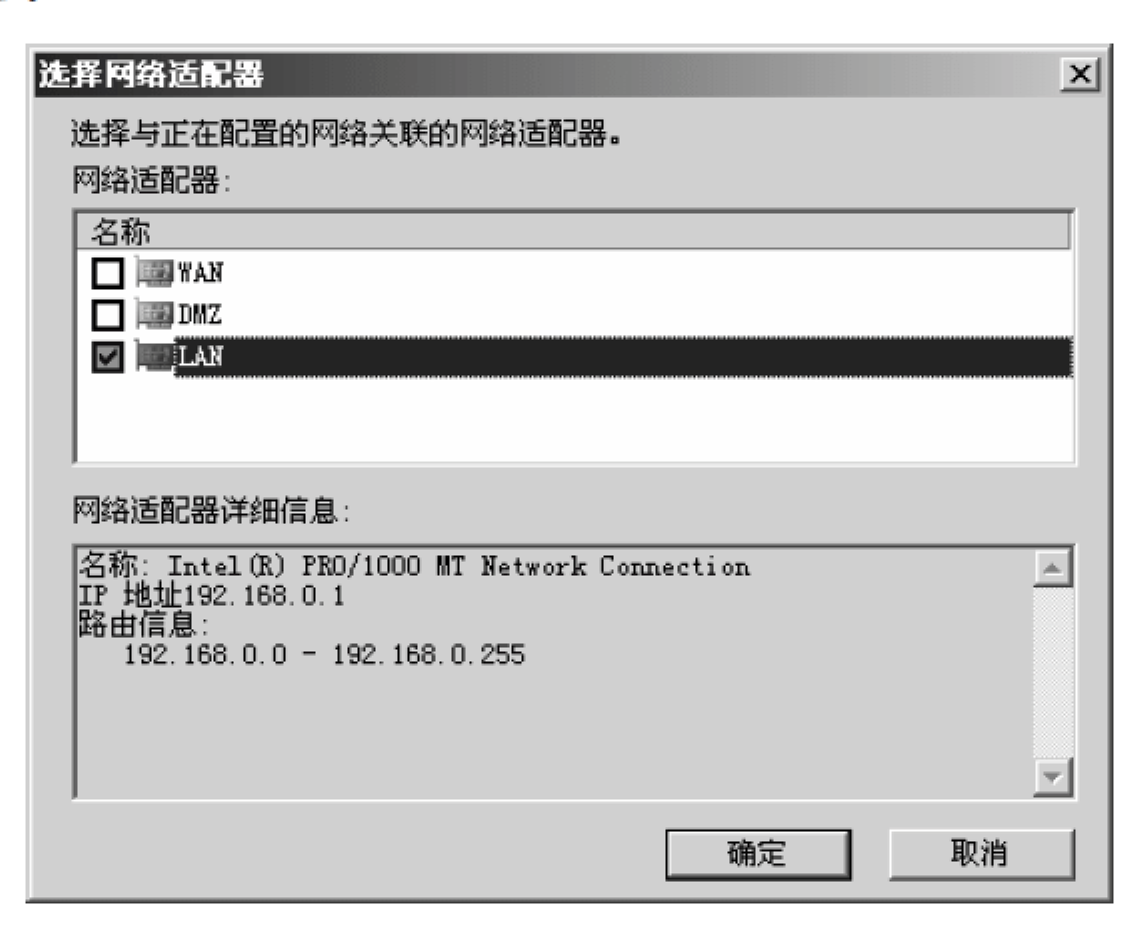


图 14-16

12 返回【地址】对话框，地址范围添加完成，单击【确定】按钮，如图 14-17 所示。

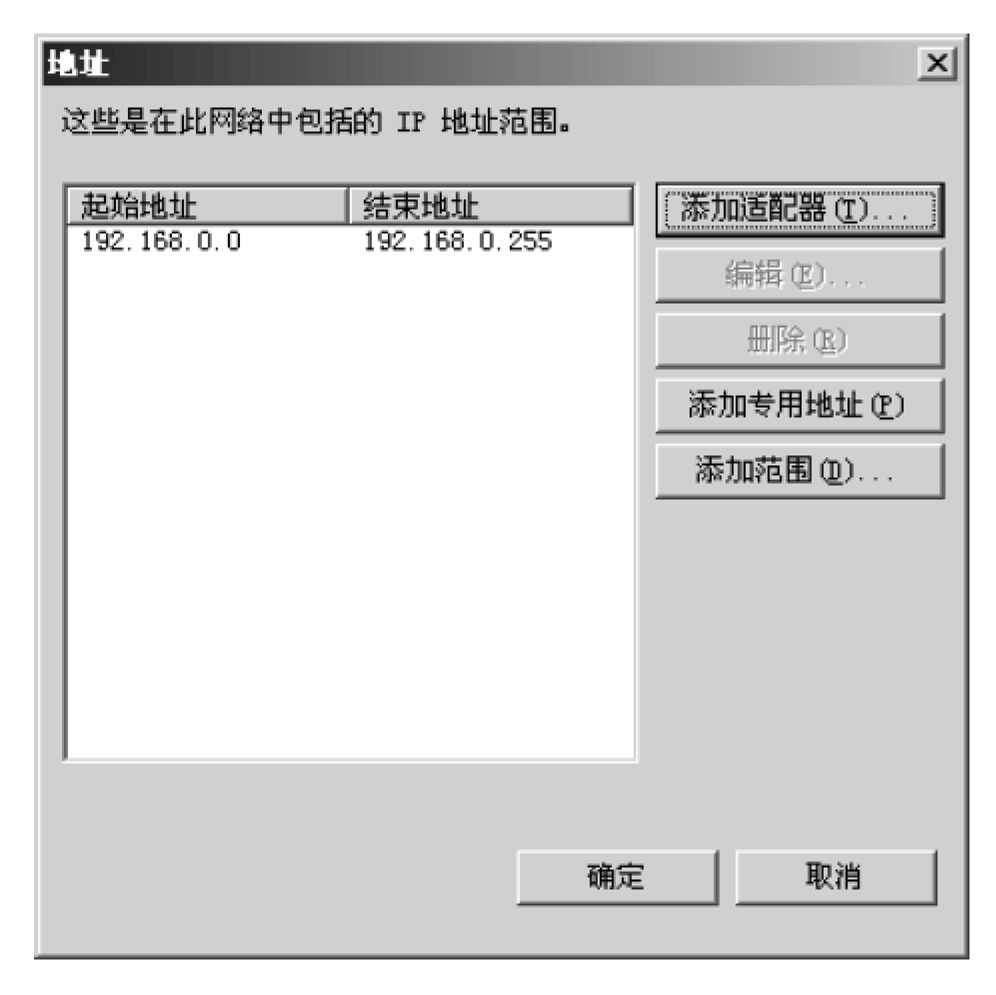


图 14-17

13 返回【内部网络】对话框，在【内部网络地址范围】窗格中显示内部地址范围，单击【下一步】按钮，如图 14-18 所示。

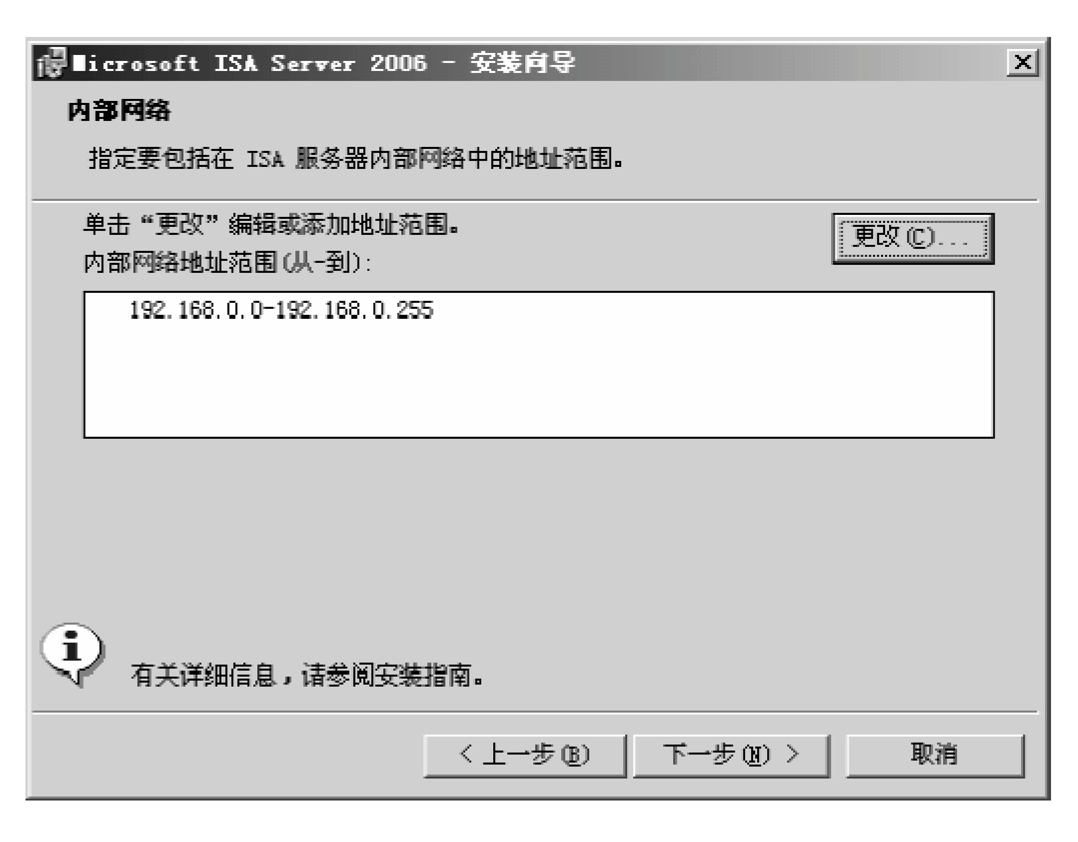


图 14-18

14 弹出【防火墙客户端连接】对话框，该对话框主要设置 ISA 对老版本系统客户端的兼容，本实例采用默认配置，如图 14-19 所示，单击【下一步】按钮。

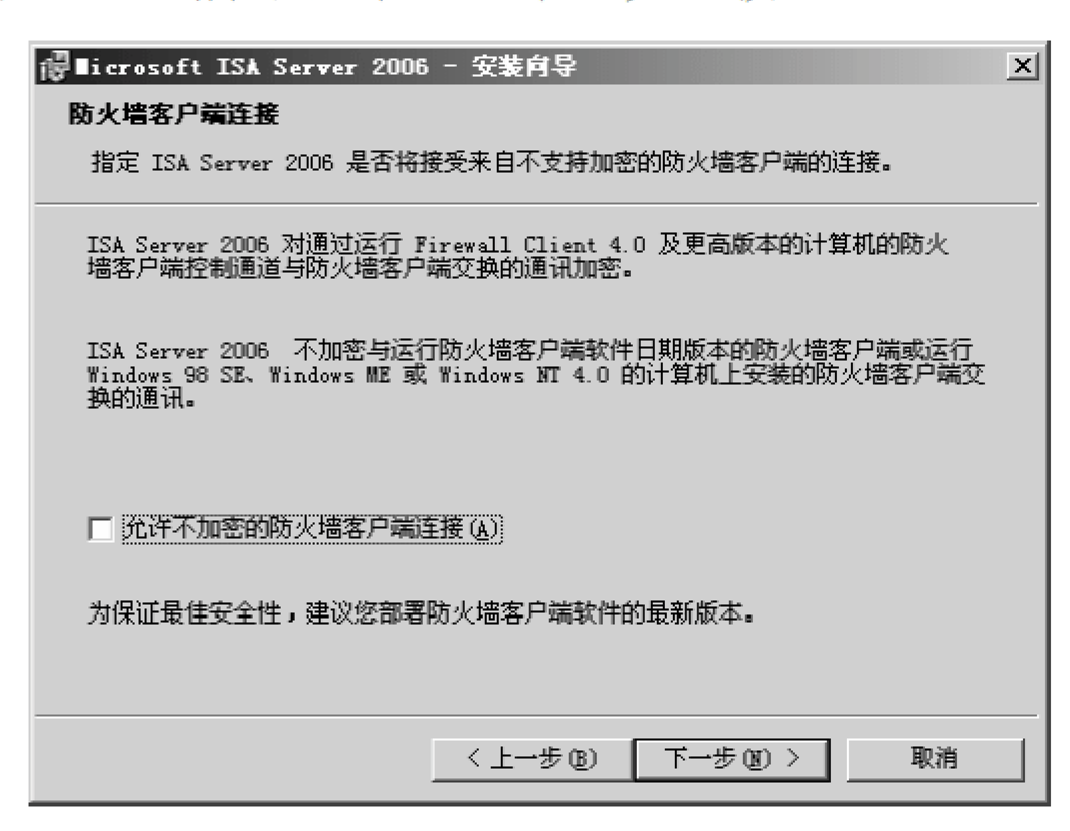


图 14-19

15 弹出【服务警告】对话框，部分系统程序会影响 ISA 程序的安装，需要在安装 ISA 时将这些服务重新启动，单击【下一步】按钮，如图 14-20 所示。

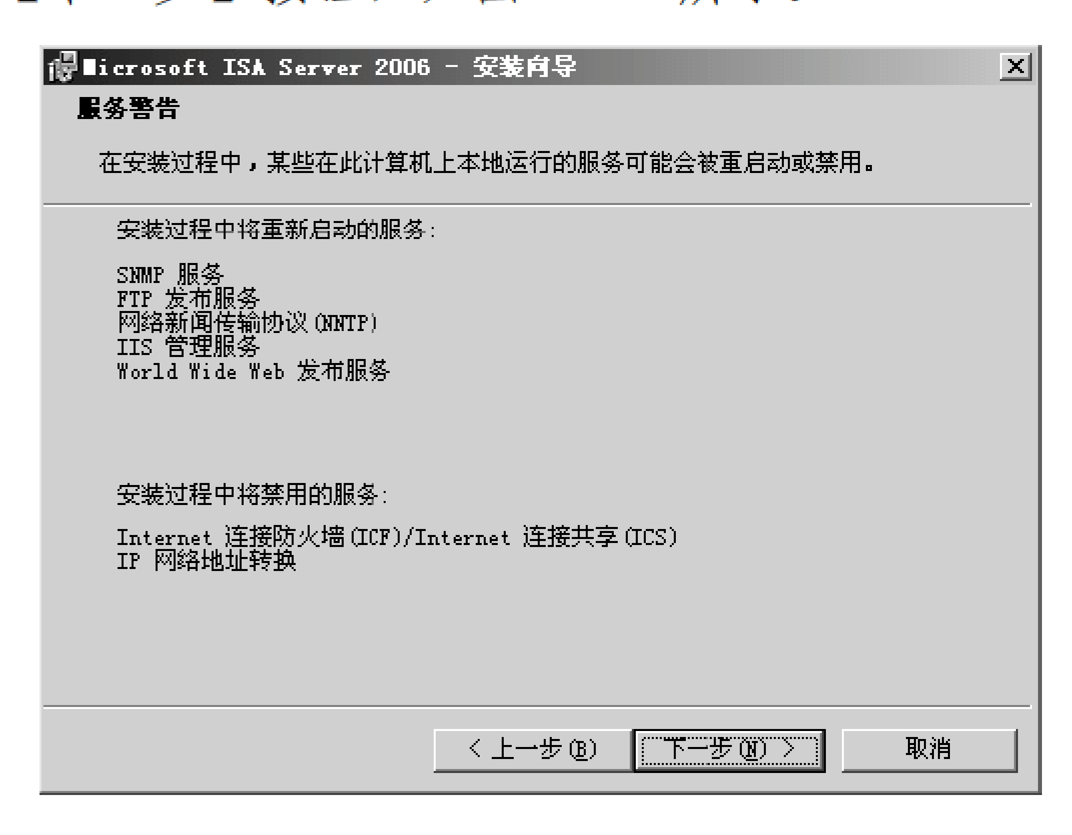


图 14-20

16 弹出【可以安装程序了】对话框，单击【安装】按钮，如图 14-21 所示。

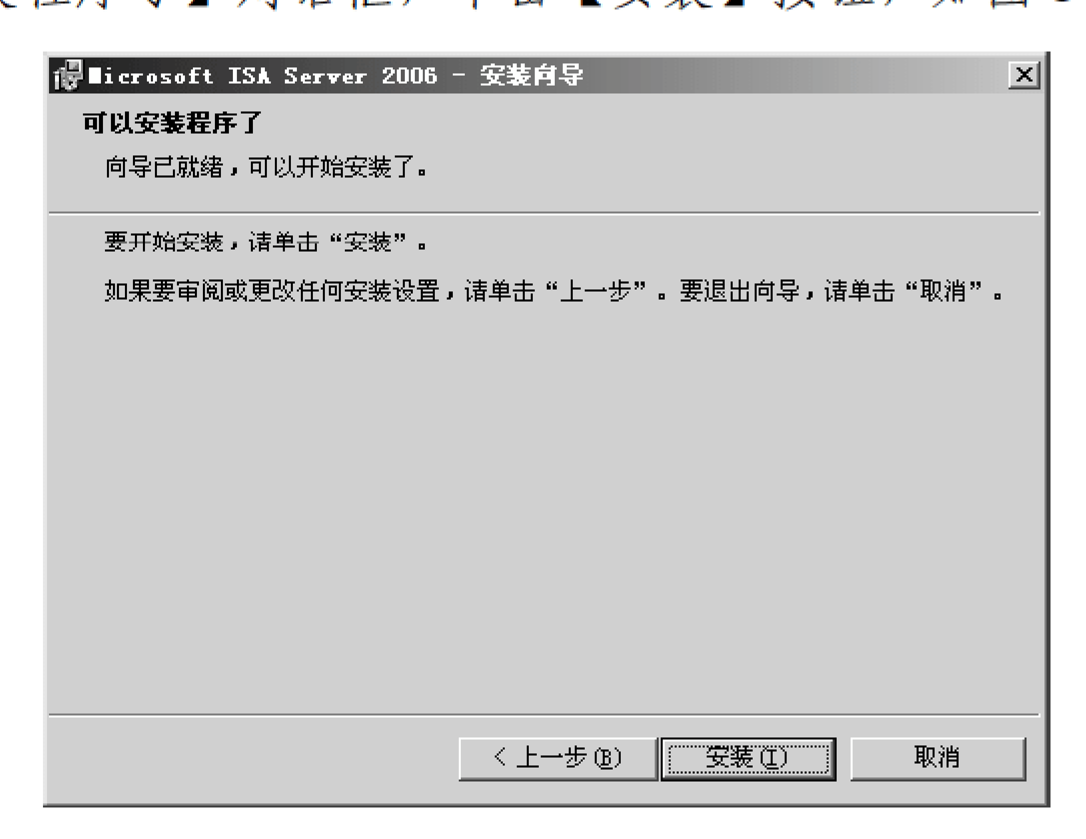


图 14-21

17 系统依照配置自动安装程序，安装完成后弹出【安装向导完成】对话框，如图 14-22 所示，单击【完成】按钮，至此 ISA 2006 已经安装成功。



图 14-22

14.2.3 添加 DMZ（隔离区），改变 ISA 联网模式

DMZ 区作为对外发布服务器的位置，需要连入 ISA 防火墙，但是默认安装完 ISA 防火墙后，并没有添加 DMZ 区的网卡，若想要把 DMZ 区网络加入 ISA 防火墙，需要手动添加。

添加 DMZ 区域的具体操作步骤如下。

01 选择【开始】➢【程序】➢【Microsoft ISA Server】➢【ISA 服务器管理】菜单命令，如图 14-23 所示，运行 ISA 防火墙。



图 14-23

02 打开程序主界面，在左侧选项列表中选择【阵列】➢【aa-6db32af13796】➢【配置】➢【网络】选项，“aa-6db32af13796”为本地服务器计算机名，右侧显示出当前 ISA 防火墙采用的是【边缘防火墙】部署结构，在右侧【模板】选项卡中显示了可用 ISA 部署结构，单击【3 向外围网络】选项，如图 14-24 所示。



图 14-24

03 弹出【网络模板向导】对话框，单击【下一步】按钮，如图 14-25 所示。



图 14-25

04 弹出【导出 ISA 服务器的配置】对话框，如果担心当前 ISA 服务器丢失，可以单击【导出】按钮将现有配置导出保存，如图 14-26 所示，单击【下一步】按钮。

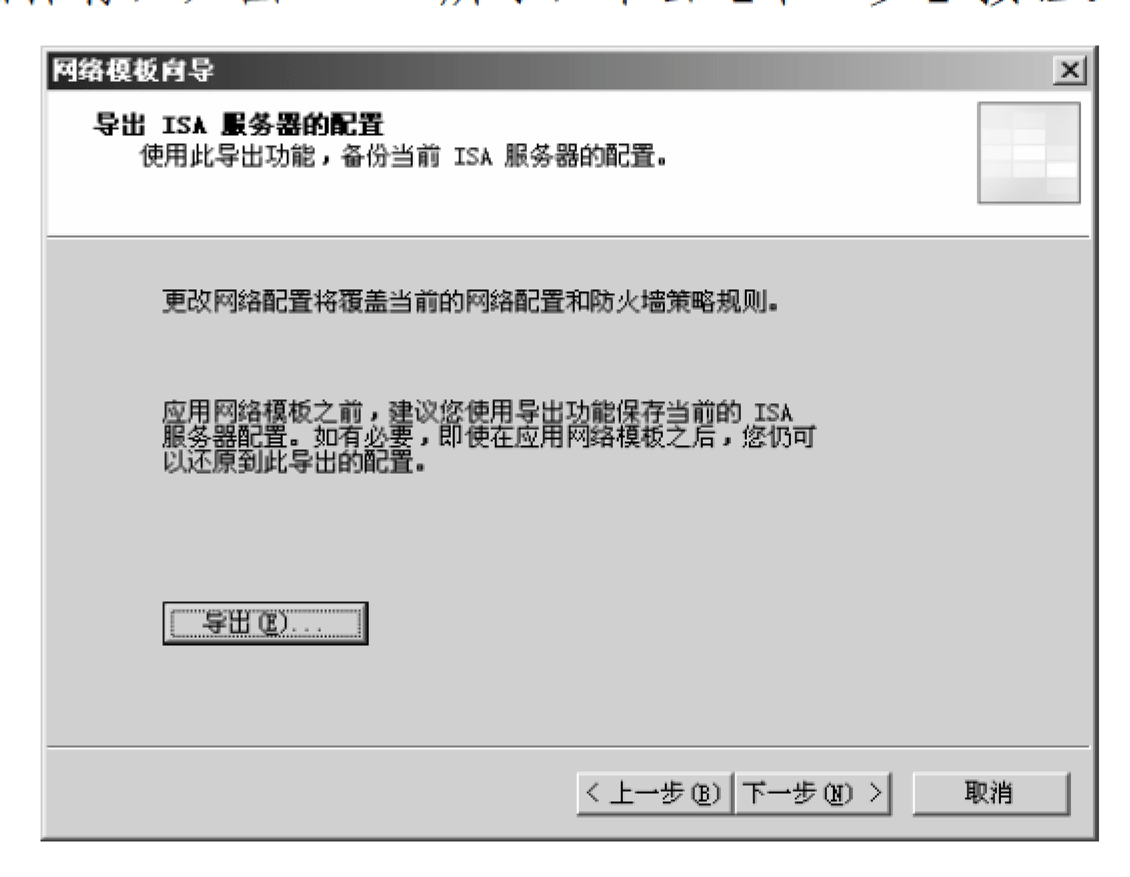


图 14-26

05 弹出【内部 网络 IP 地址】对话框，安装防火墙时此项配置已经操作，如图 14-27 所示，单击【下一步】按钮。

网络模板向导
内部 网络 IP 地址
请指定此网络的 IP 地址。您可以添加 IP 地址范围、与此网卡关联的 IP 地址范围和专用 IP 范围。
地址范围:

起始地址	结束地址
192.168.0.0	192.168.0.255

添加适配器(D)...　编辑(E)...　删除(R)　添加专用地址(P)　添加范围(A)...
企业网络:
添加网络(T)...
< 上一步(B)　下一步(N) >　取消

图 14-27

06 弹出【外围 网络 IP 地址】对话框，“外围网络”就是“DMZ 区”，单击【添加适配器】按钮，如图 14-28 所示。

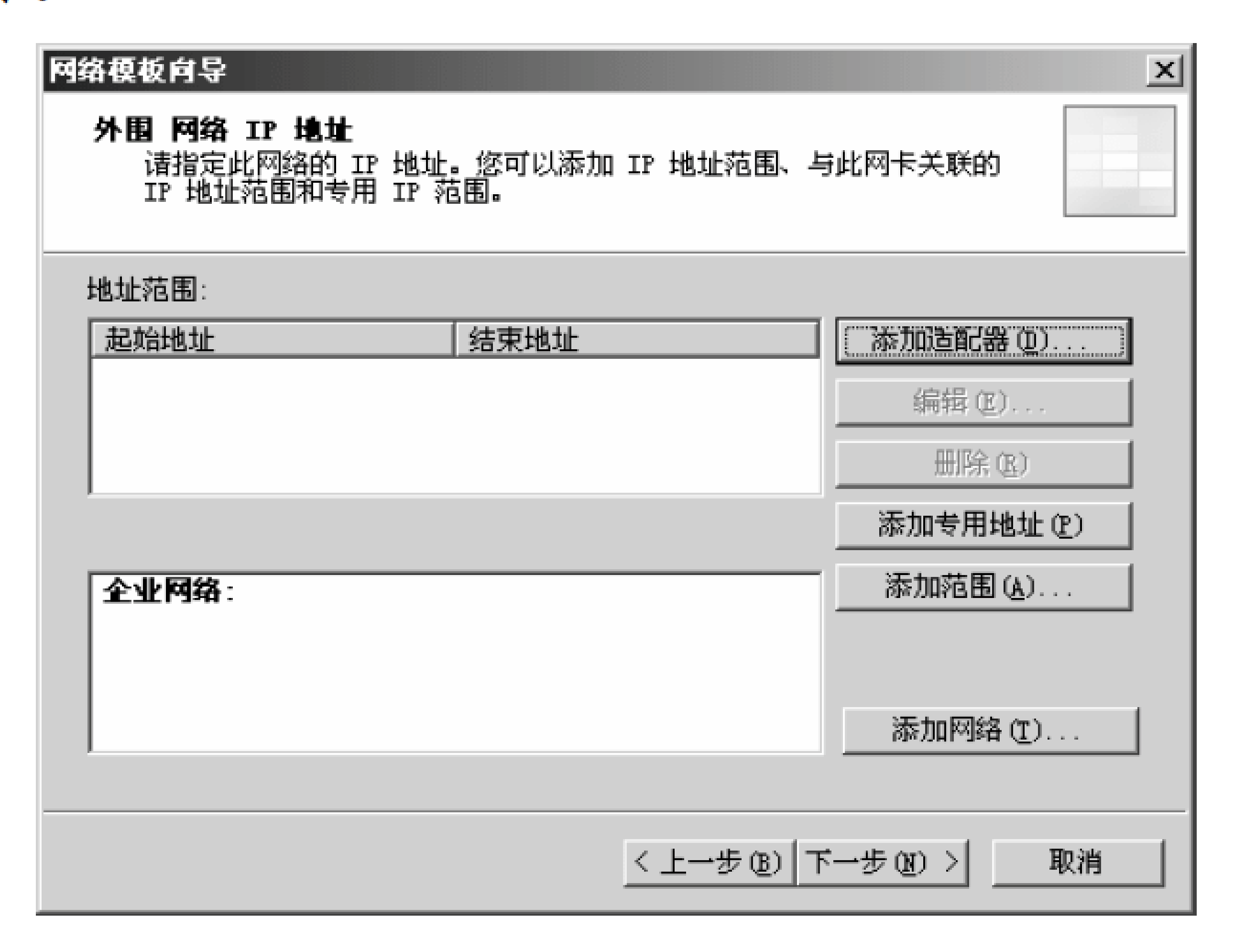


图 14-28

07 弹出【选择网络适配器】对话框，在【网络适配器】选项列表中选择【DMZ】复选框，如图 14-29 所示，单击【确定】按钮。

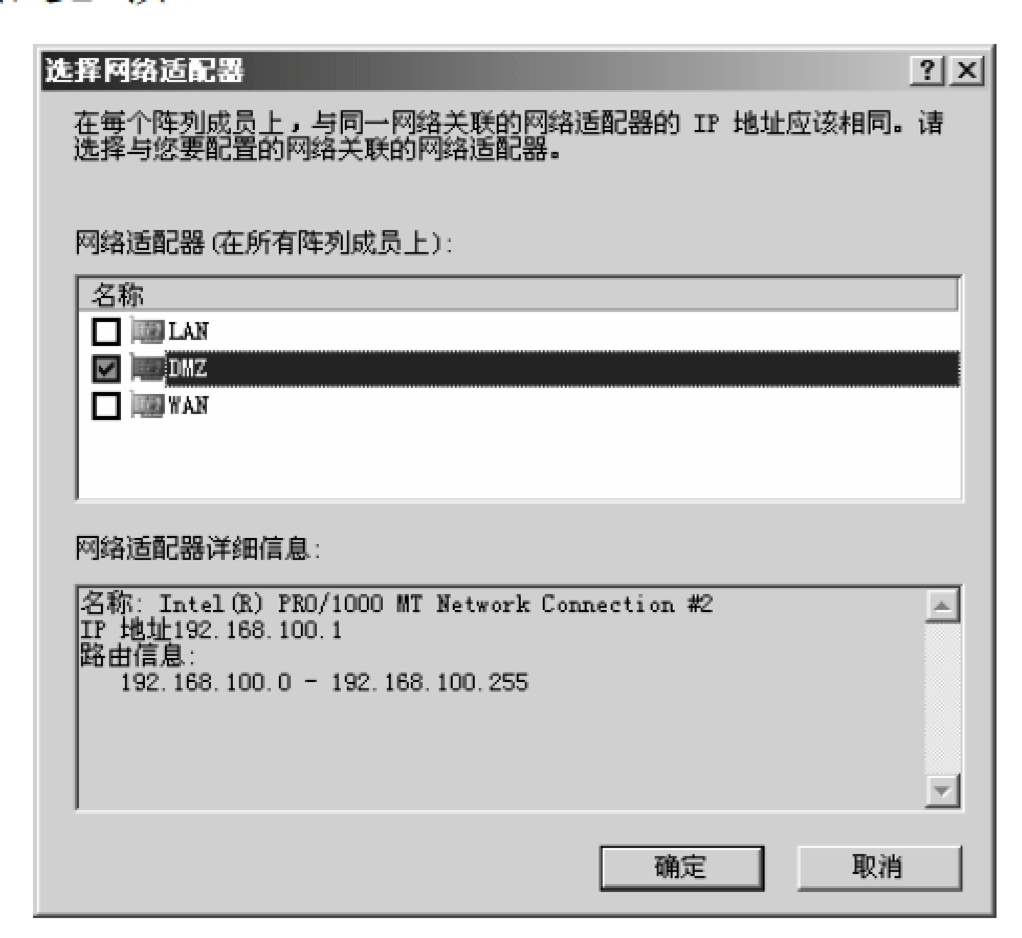


图 14-29

08 返回【外围 网络 IP 地址】对话框，在【地址范围】窗格中显示 DMZ 区的网络地址范围，如图 14-30 所示，单击【下一步】按钮。

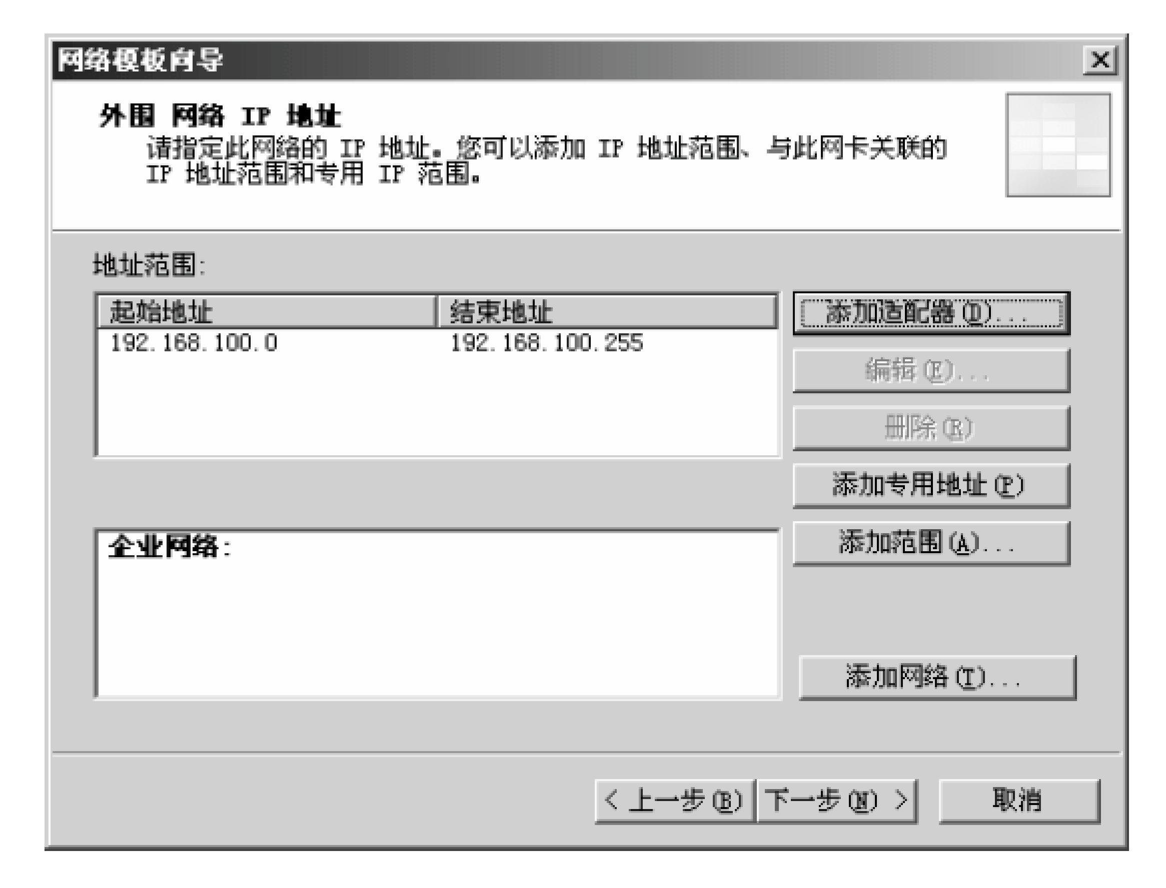


图 14-30

09 弹出【选择一个防火墙策略】对话框，在此可以选择防火墙默认使用的控制策略，一般选择【阻止所有访问】选项，如图 14-31 所示，单击【下一步】按钮。

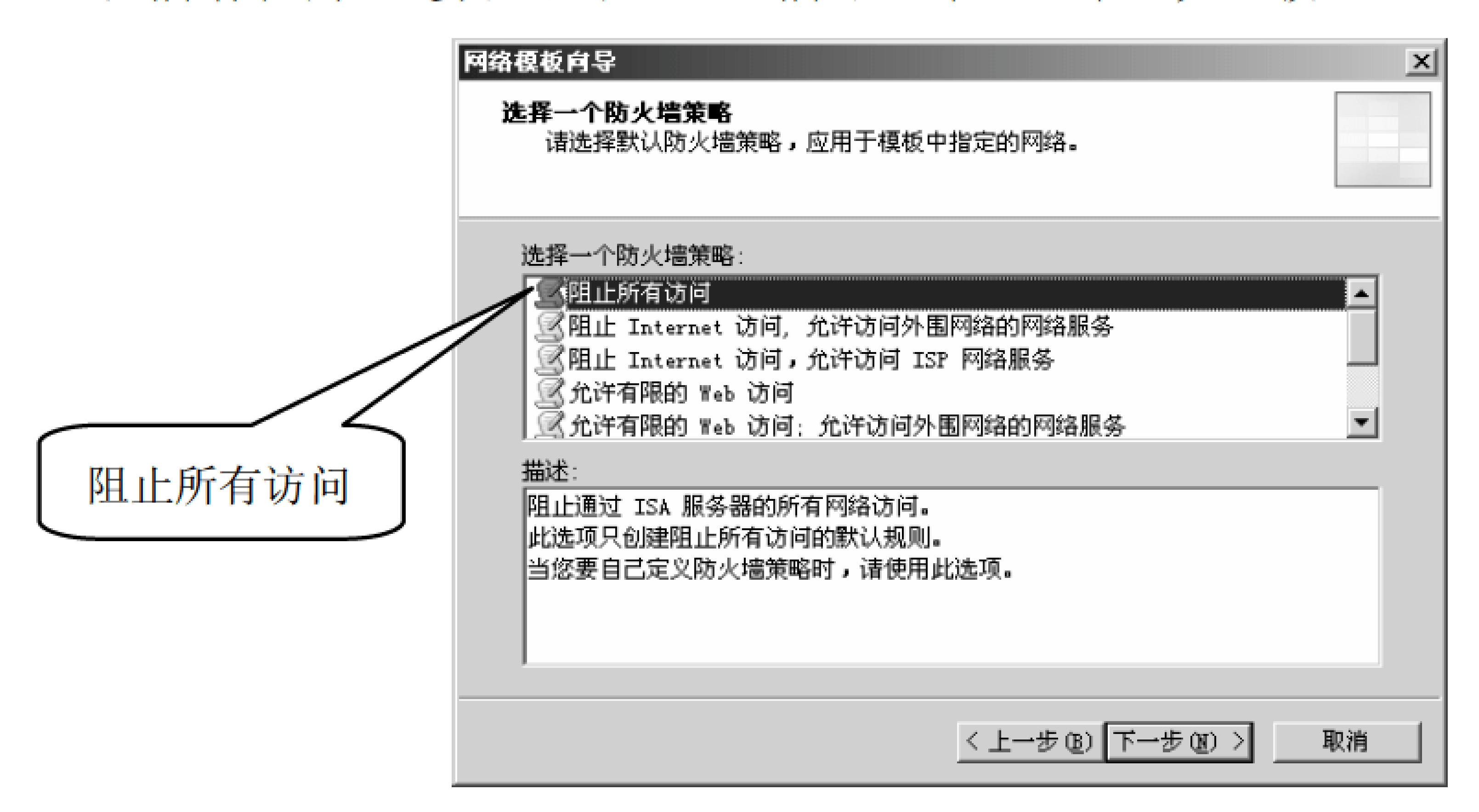


图 14-31

10 配置完成，在弹出的对话框中显示了新 ISA 部署结构的配置信息，如图 14-32 所示，单击【完成】按钮。

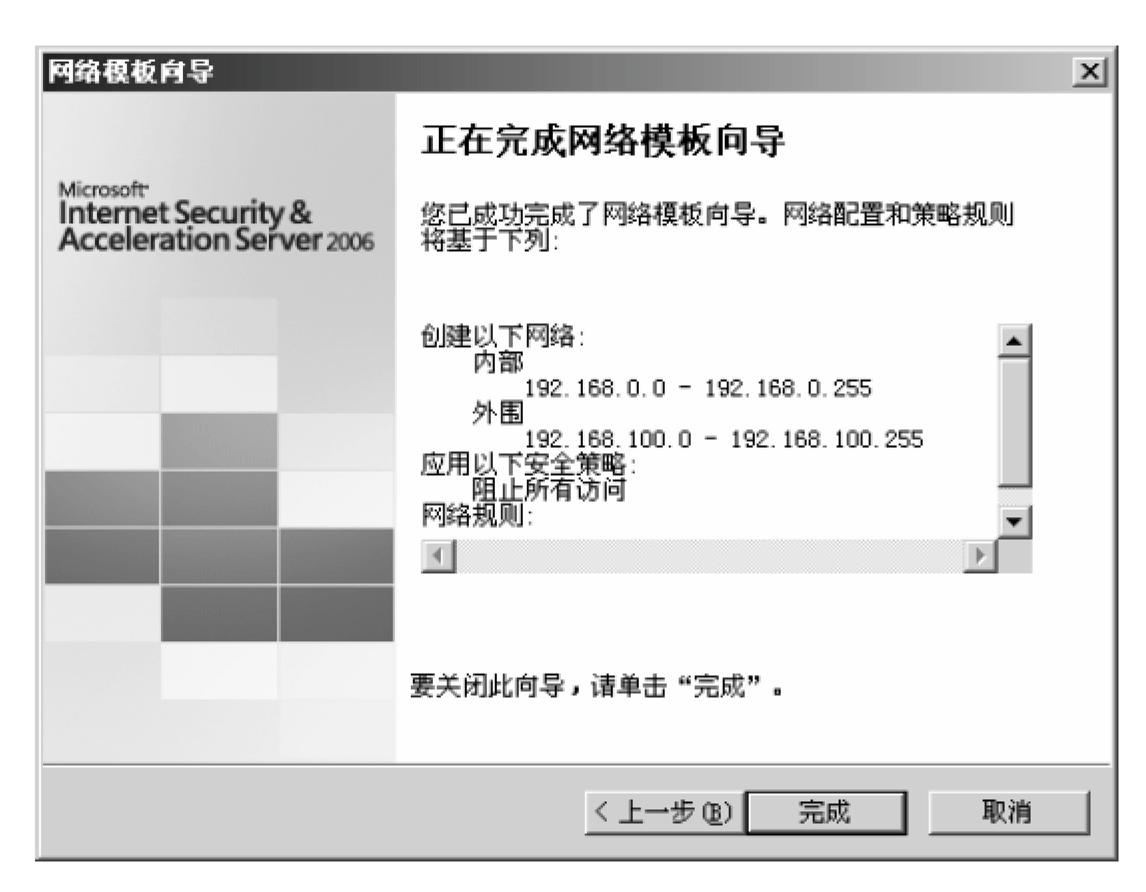


图 14-32

11 在 ISA 程序主界面显示了调整后的部署结构图，单击【应用】按钮，应用本次修改，如图 14-33 所示。

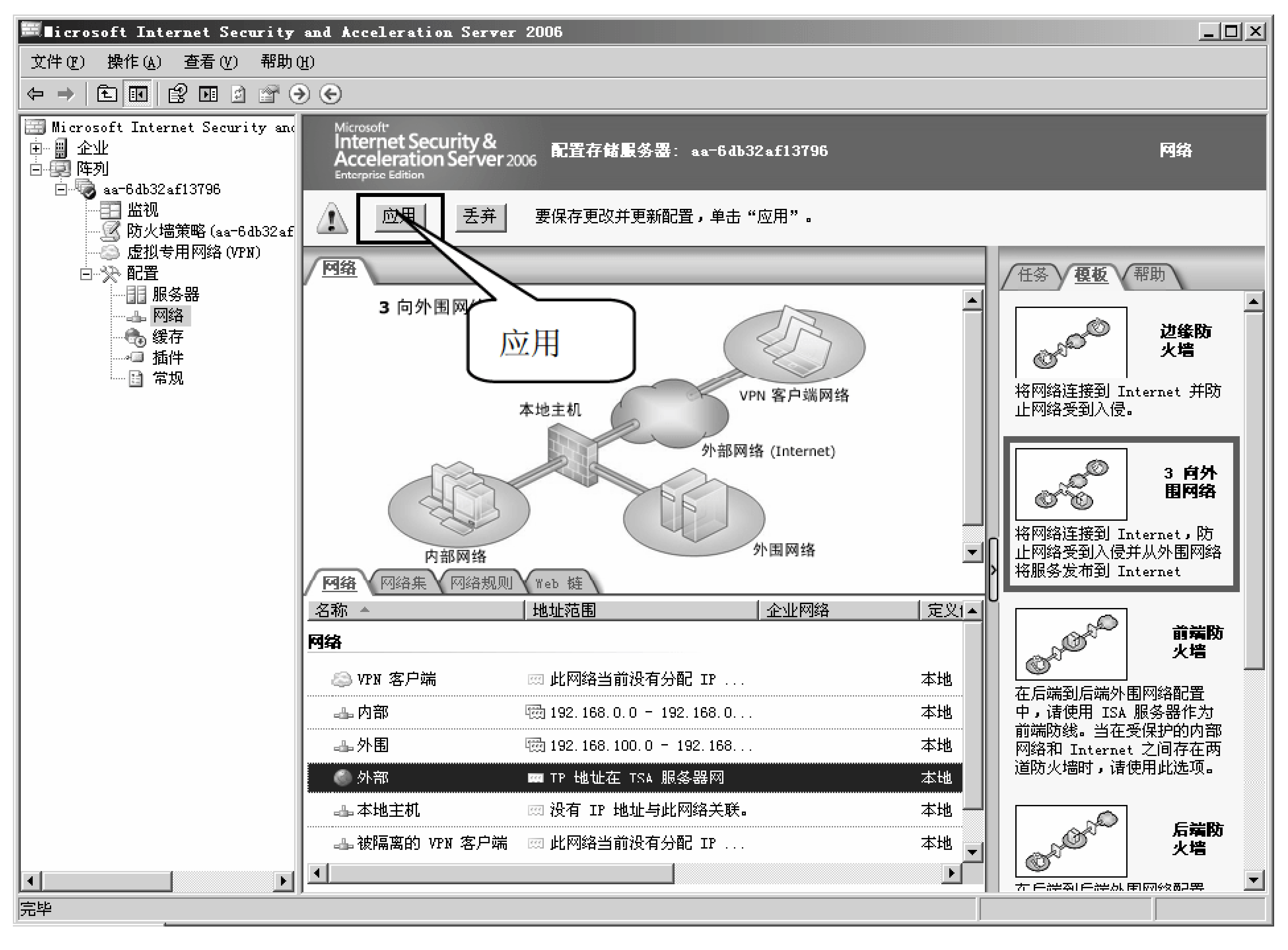


图 14-33

12 弹出【正在保存配置更改】对话框，保存完成后，单击【确定】按钮，如图 14-34 所示。

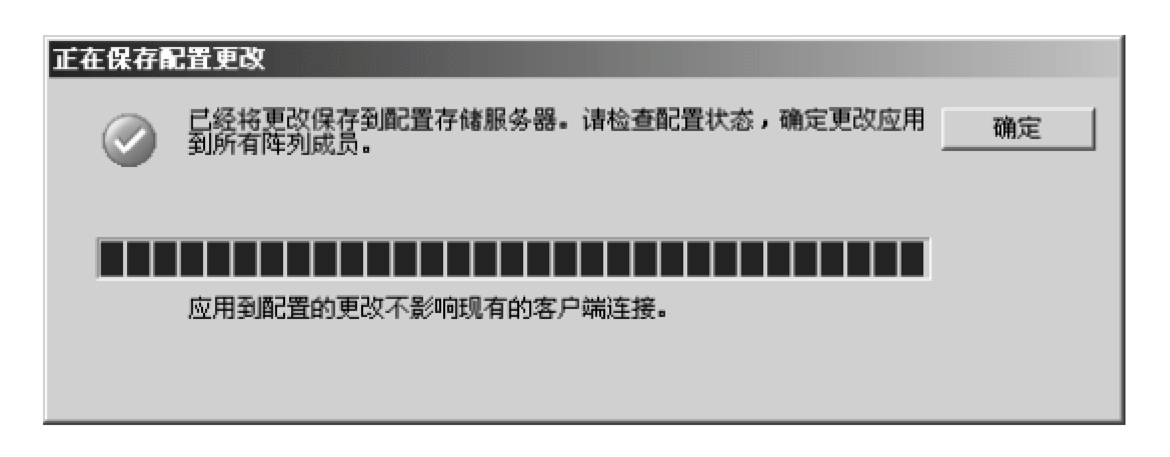


图 14-34

13 配置保存后并不能马上生效，ISA 服务器配置需要和存储配置服务器同步，在左侧选项列表中选择【监视】选项，在右侧窗格中选择【配置】选项卡，刚应用的配置尚未同步，单击右侧【任务】选项卡的【现在刷新】按钮，如图 14-35 所示，可以马上完成配置同步。



图 14-35

除了使用以上方法更换新的部署结构外，也可以通过在现有部署结构上直接增加“新网络”的方式，完成 DMZ 区的添加，具体操作步骤如下。

01 在左侧选项列表中选择【阵列】➢【aa-6db32af13796】➢【配置】➢【网络】选项，单击右侧【任务】选项卡下的【创建一个新的网络】选项，如图 14-36 所示。

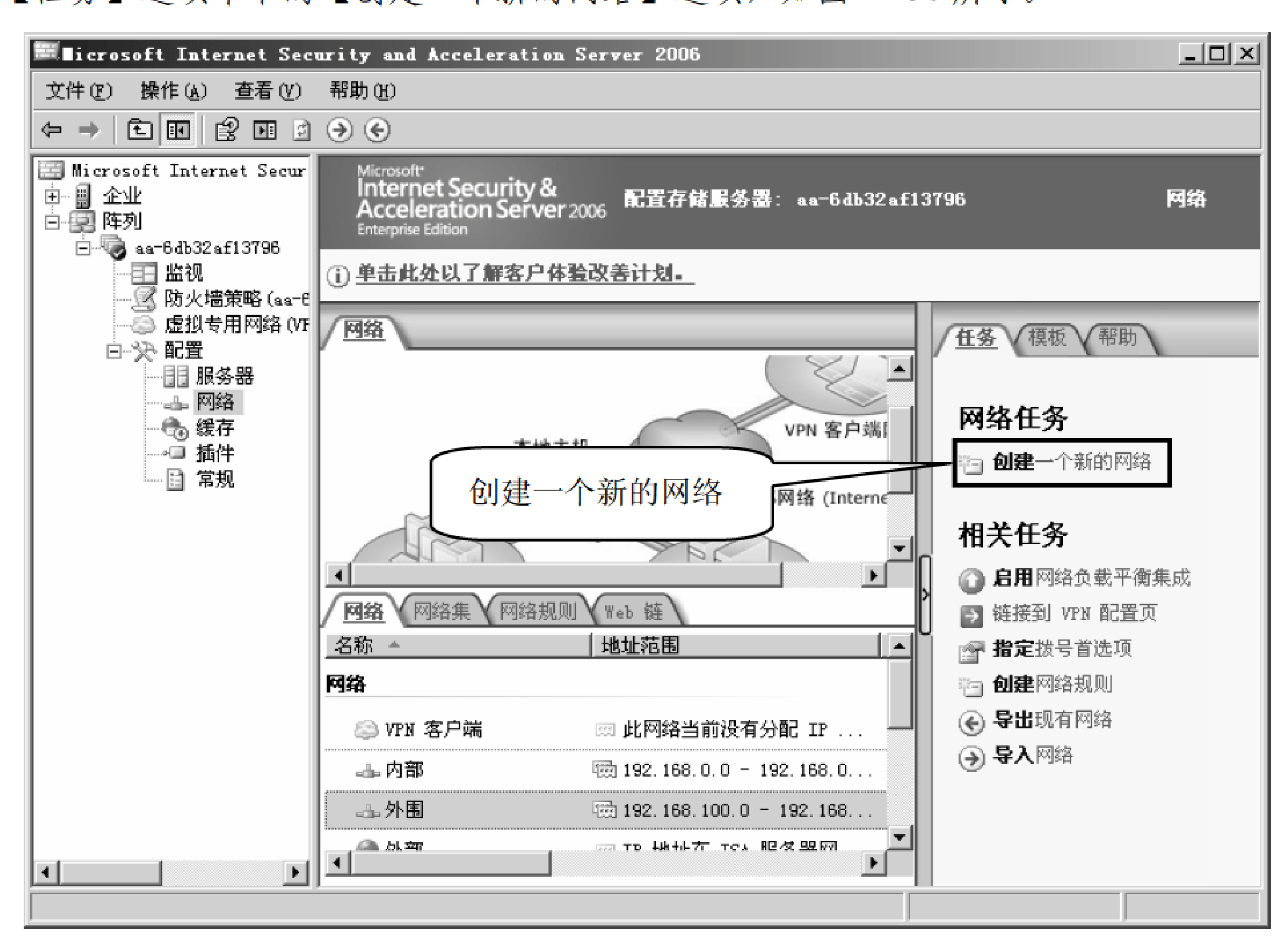


图 14-36

02 弹出【新建网络向导】对话框，在【网络名】文本框中输入“DMZ” ，如图 14-37 所示，单击【下一步】按钮。

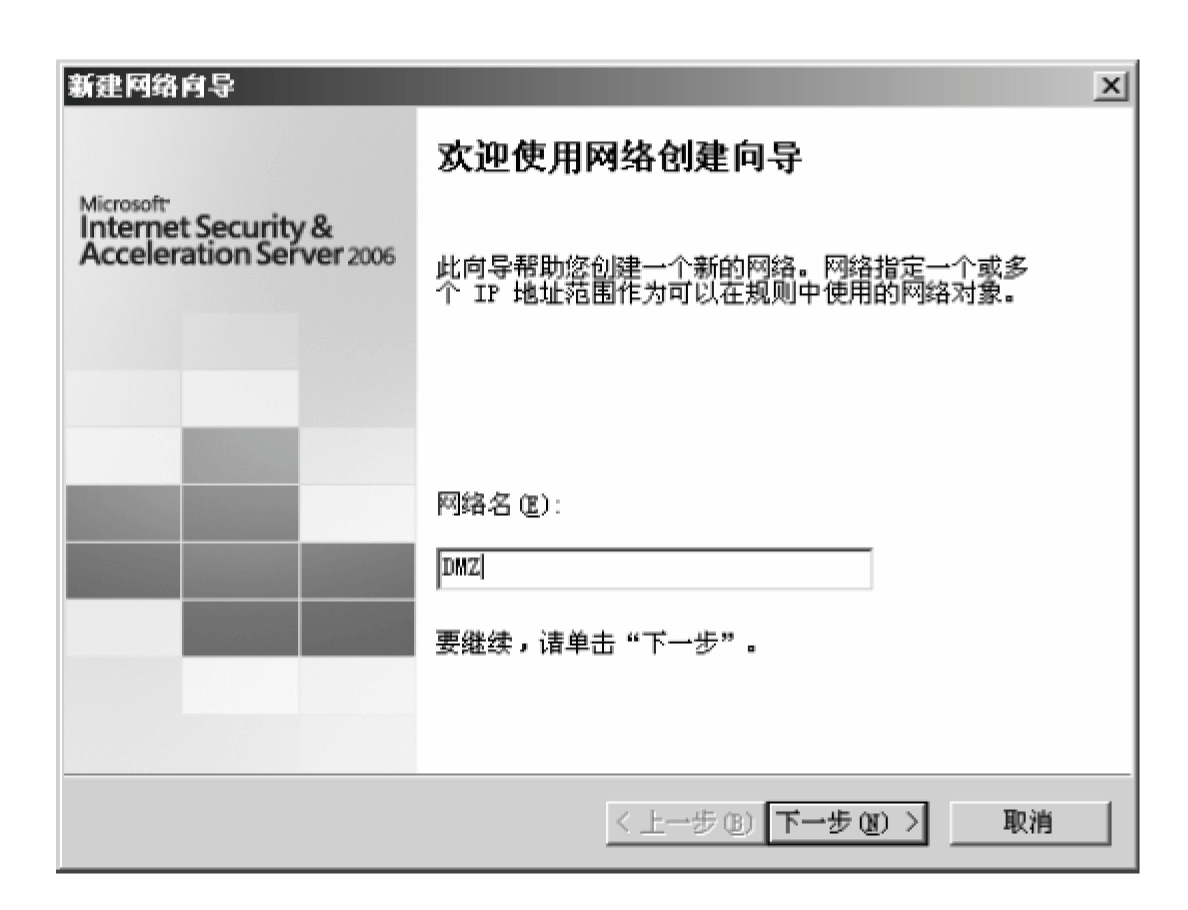


图 14-37

03 弹出【网络类型】对话框，选择【外围网络】单选按钮，如图 14-38 所示，单击【下一步】按钮。

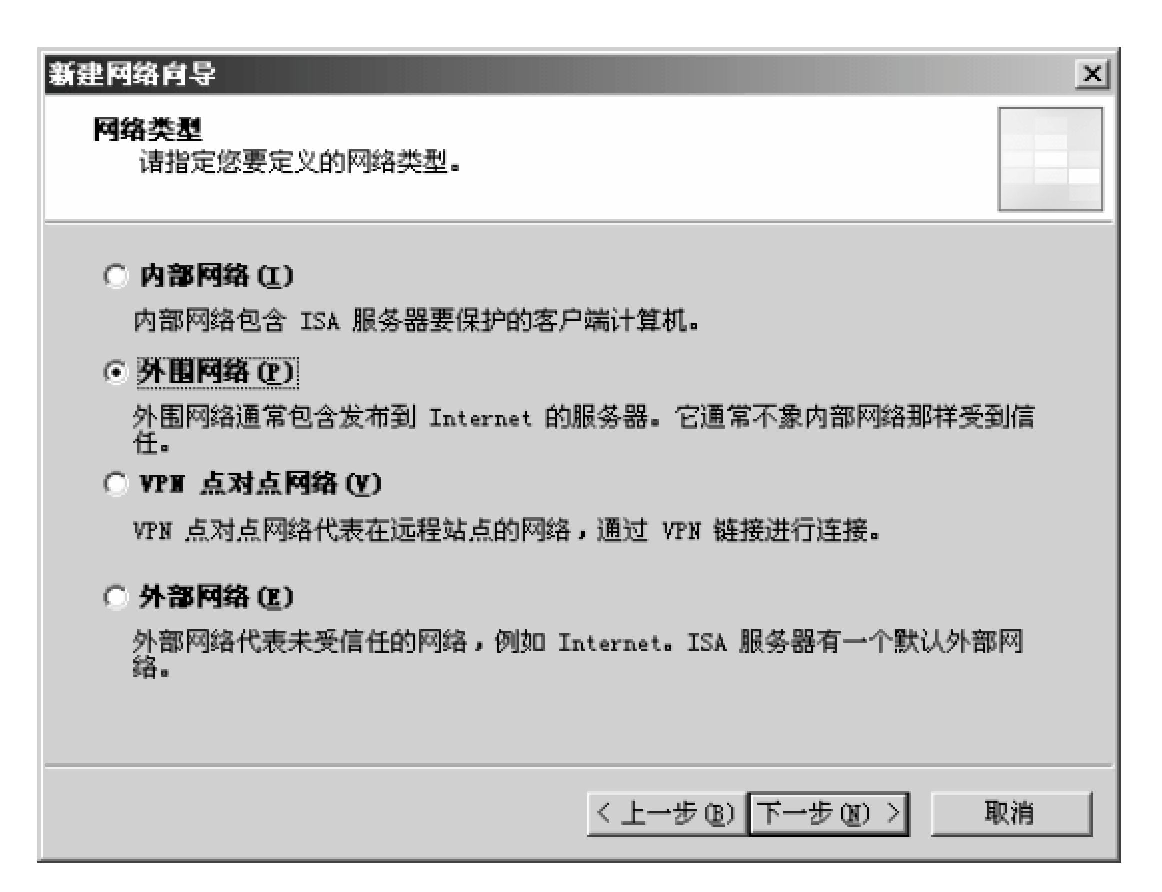


图 14-38

04 弹出【网络地址】对话框，单击【添加适配器】按钮，选择 DMZ 区连接的网卡，如图 14-39 所示。



图 14-39



以下操作步骤与第一种操作方法类似，这里不再详细描述。

14.3 项目实施 2：利用 ISA 控制员工上网

由于工作需求，很多企业对员工的上网行为都有所约束，特别是像 QQ 空间、开心网、迅雷看看等娱乐型的网站，都会影响到员工的工作效率。因此，在架设 ISA 防火墙时，必须要准确控制员工的上网行为，具体控制方法及内容有以下几点。

14.3.1 允许员工访问互联网

由于业务需求，员工必须要有一定的网络访问权限。一般访问网络需要开启 HTTP、DNS、POP3、SMTP 等服务，具体操作步骤如下。

01 打开程序主界面，在左侧选项列表中选择【防火墙策略】选项，在右侧【任务】选项卡中选择【创建访问规则】选项，如图 14-40 所示。



图 14-40

02 弹出【新建访问规则向导】对话框，在【访问规则名称】文本框中输入“允许员工访问外网 WEB/MAIL/DNS 服务器”，如图 14-41 所示，单击【下一步】按钮。

03 弹出【规则操作】对话框，选择【允许】单选按钮，以确保指定流量被允许通过 ISA 防火墙，如图 14-42 所示，单击【下一步】按钮。

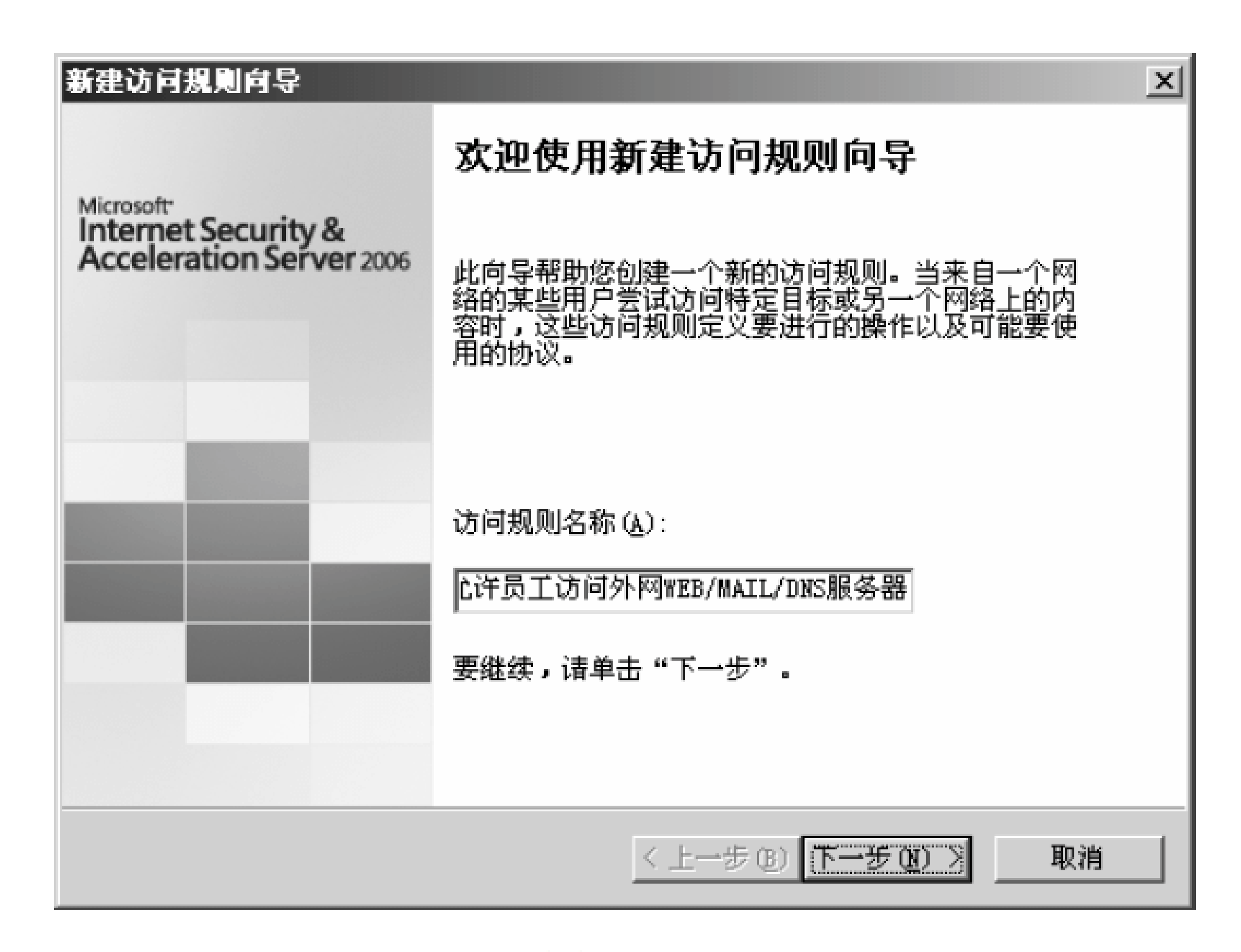


图 14-41

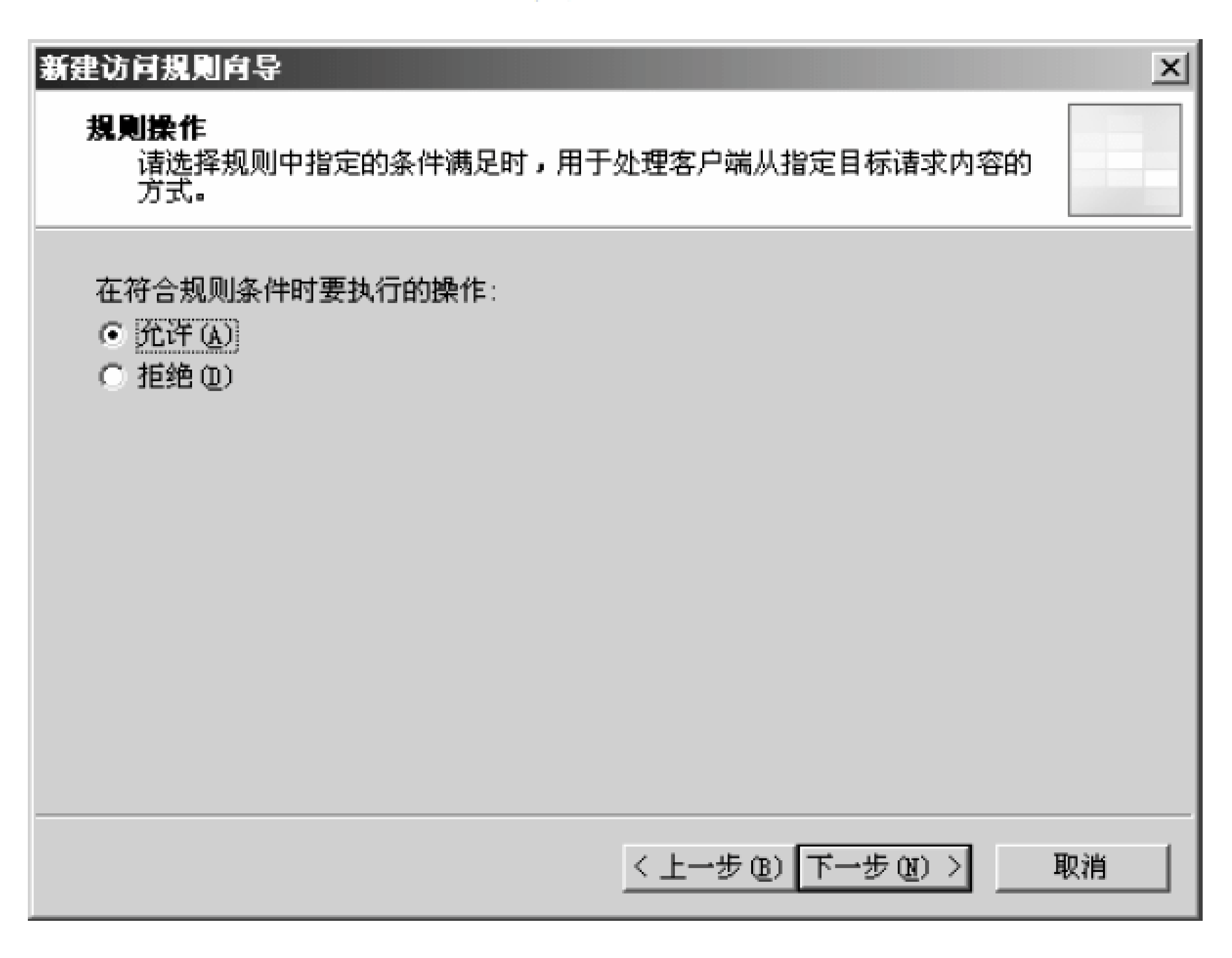


图 14-42

04 弹出【协议】对话框，在【此规则应用到】下拉列表中选择【所选的协议】选项，单击【添加】按钮，如图 14-43 所示。



图 14-43

05 弹出【添加协议】对话框，在【协议】列表中对协议进行了分类，选择 HTTP、DNS、HTTPS、POP3、SMTP 等协议，如图 14-44 所示，分别单击【添加】按钮。



图 14-44

06 返回【协议】对话框，协议添加成功，通过【编辑】按钮可以对指定协议进行编辑，单击【端口】按钮可以添加允许通过的端口范围，本实例不采用端口操作，单击【下一步】按钮，如图 14-45 所示。



图 14-45

07 弹出【访问规则源】对话框，单击【添加】按钮，如图 14-46 所示。



图 14-46

08 弹出【添加网络实体】对话框，选择【网络】➢【内部】选项，单击【添加】按钮，如图 14-47 所示。



图 14-47

09 返回【访问规则源】对话框，“内部”代表内网，即员工所在网络，如图 14-48 所示，单击【下一步】按钮。

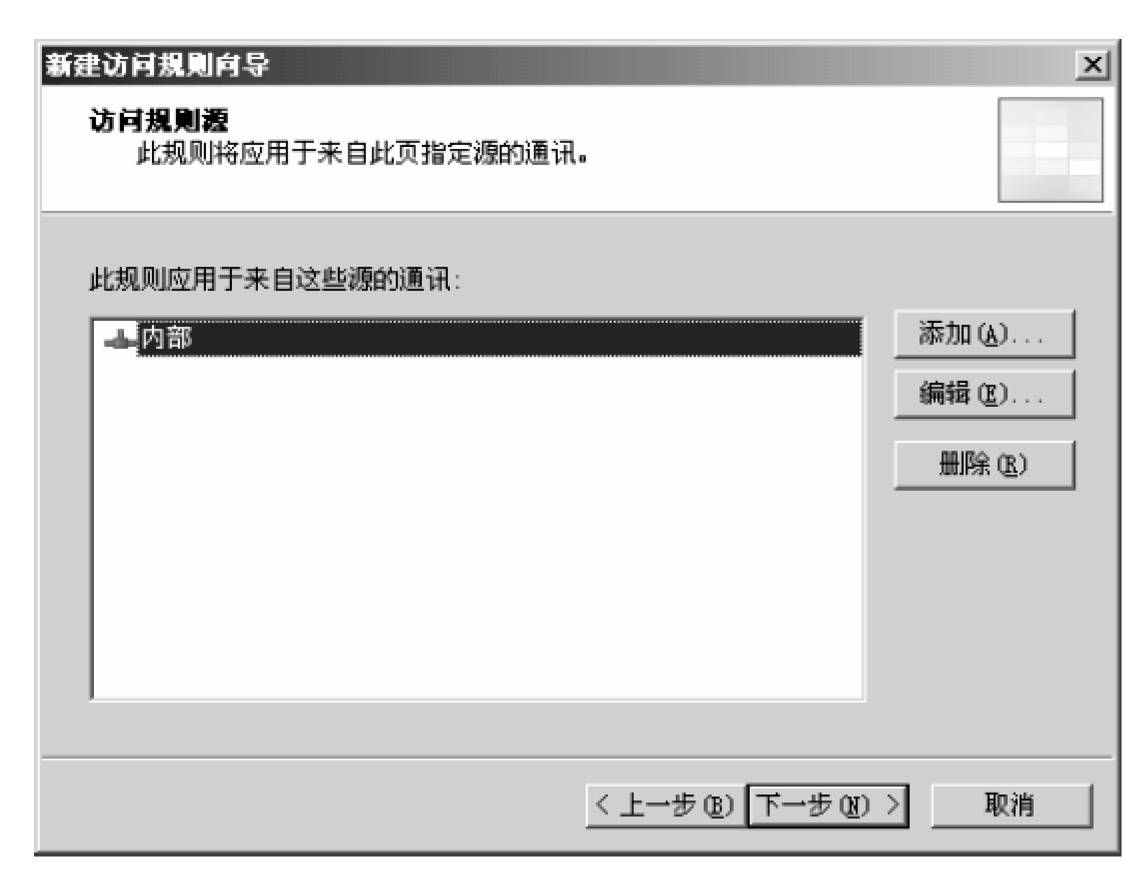


图 14-48

10 弹出【访问规则目标】对话框，单击【添加】按钮，由于员工需要有权限访问公网服务器和 DMZ 区服务器，所以要将“外围”和“外部”网络都加入访问规则目标，如图 14-49 所示，单击【下一步】按钮。

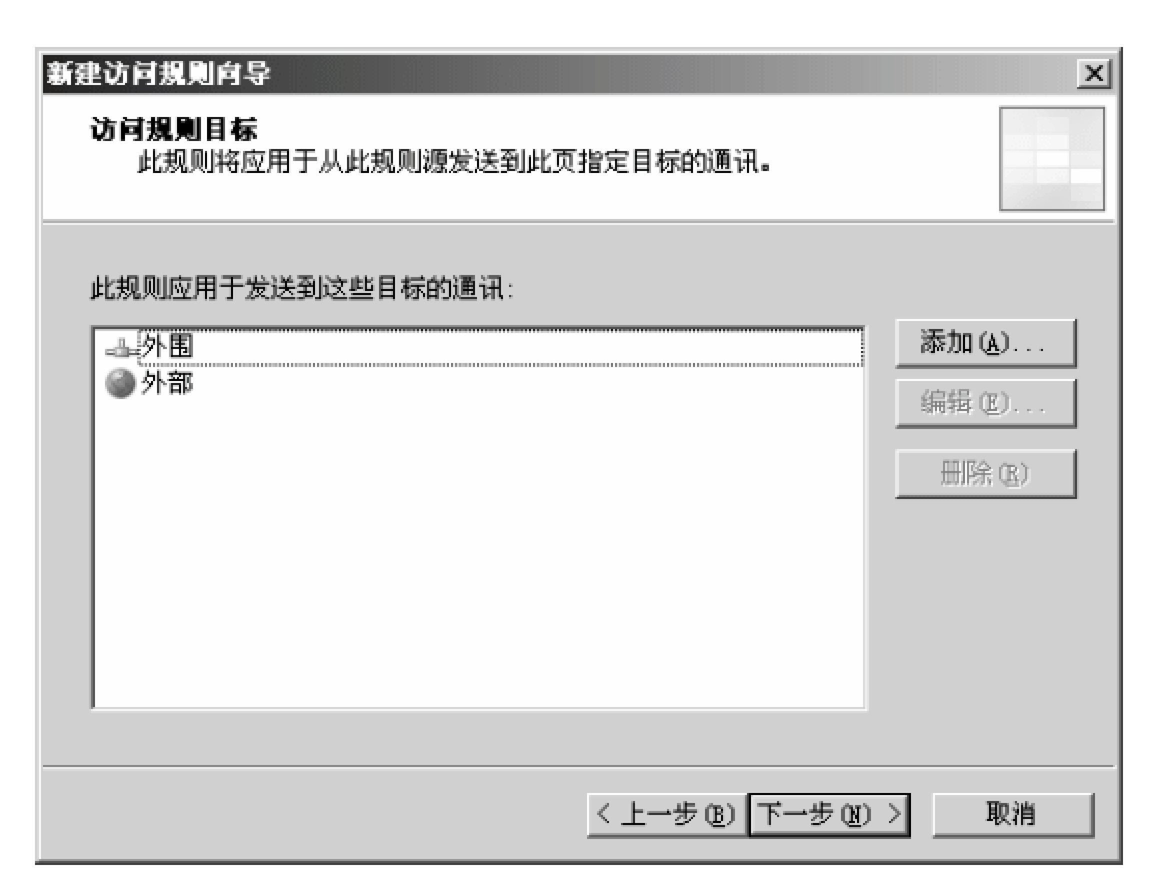


图 14-49

11 弹出【用户集】对话框，可以指定有权限使用该规则的用户，本实例采用【所有用户】，单击【下一步】按钮，如图 14-50 所示。

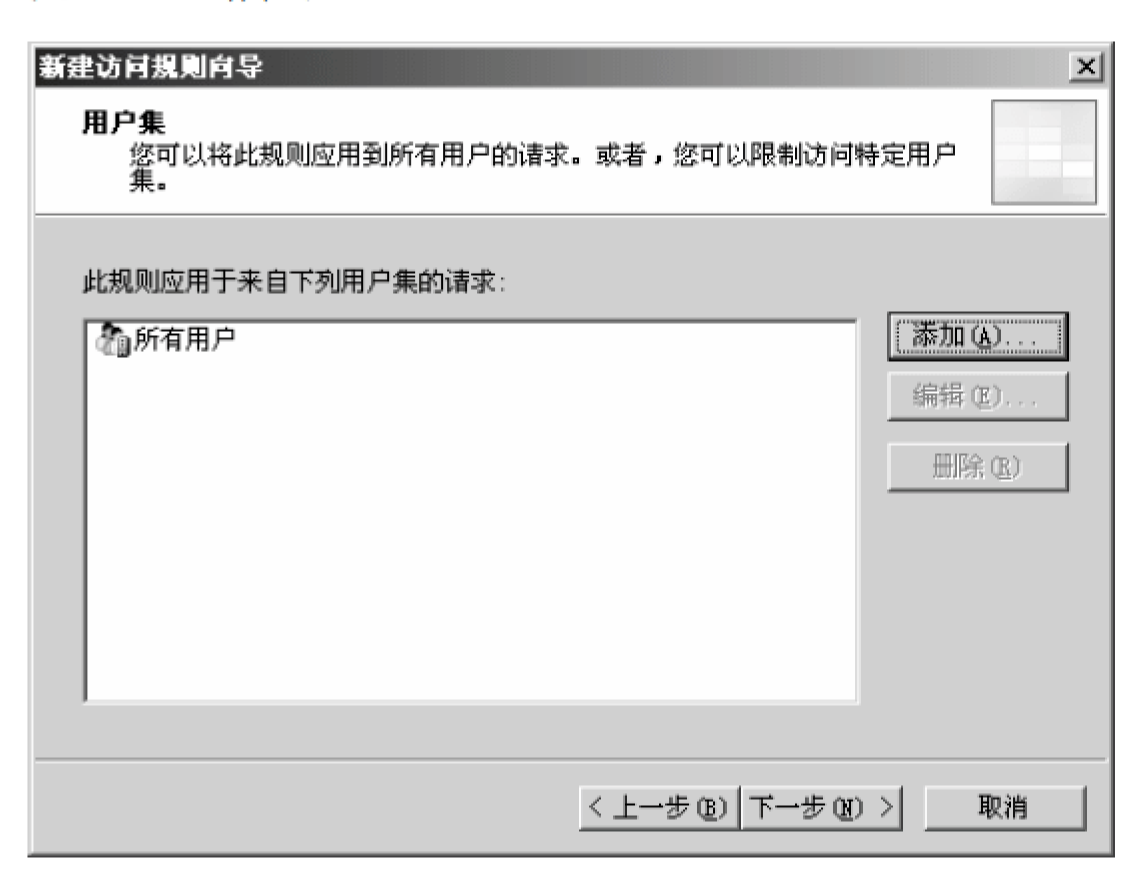


图 14-50

12 配置完成，在弹出的对话框中显示了允许员工访问公网的配置信息，如图 14-51 所示，单击【完成】按钮。

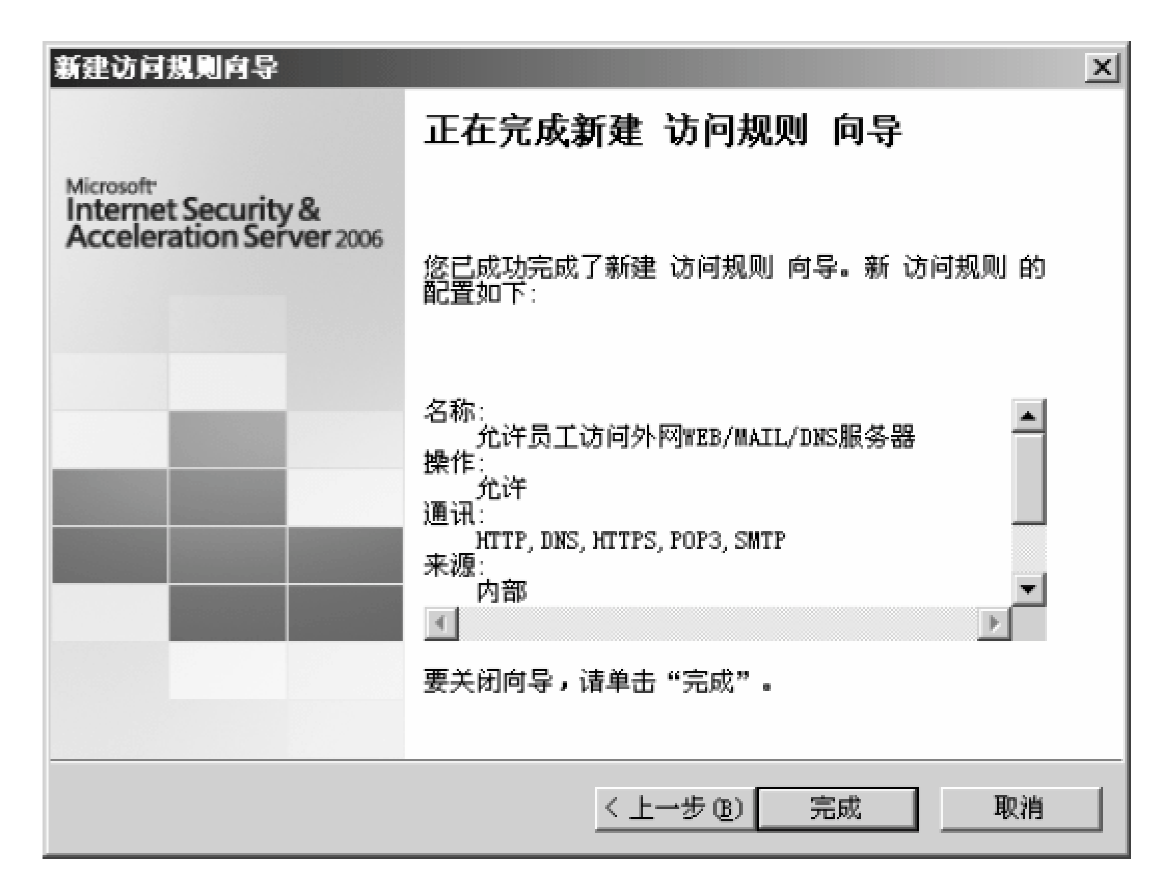


图 14-51

13 返回 ISA 防火墙主界面，在【防火墙策略】窗格中显示了新添加的访问规则，单击【应用】按钮，使配置生效，如图 14-52 所示。

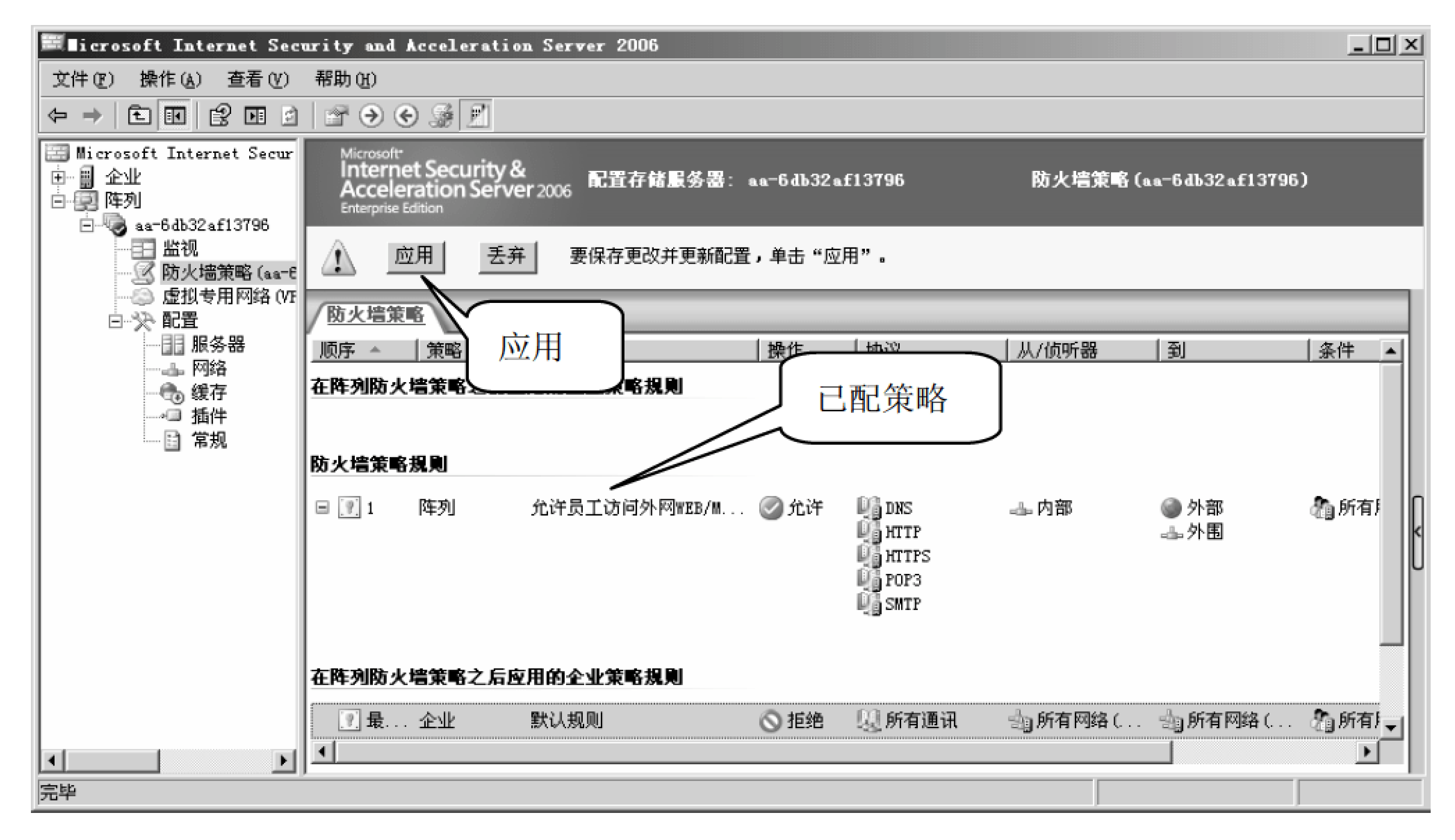


图 14-52

14.3.2 限制员工的上网时间

考虑到工作需要，可以限制员工上网时间段，具体操作步骤如下。

01 右击允许员工访问网络的策略，在弹出的快捷菜单中选择【属性】菜单命令，如图 14-53 所示。



图 14-53

02 弹出策略属性，选择【计划】选项卡，默认该策略总是生效，如图 14-54 所示，单击【新建】按钮。

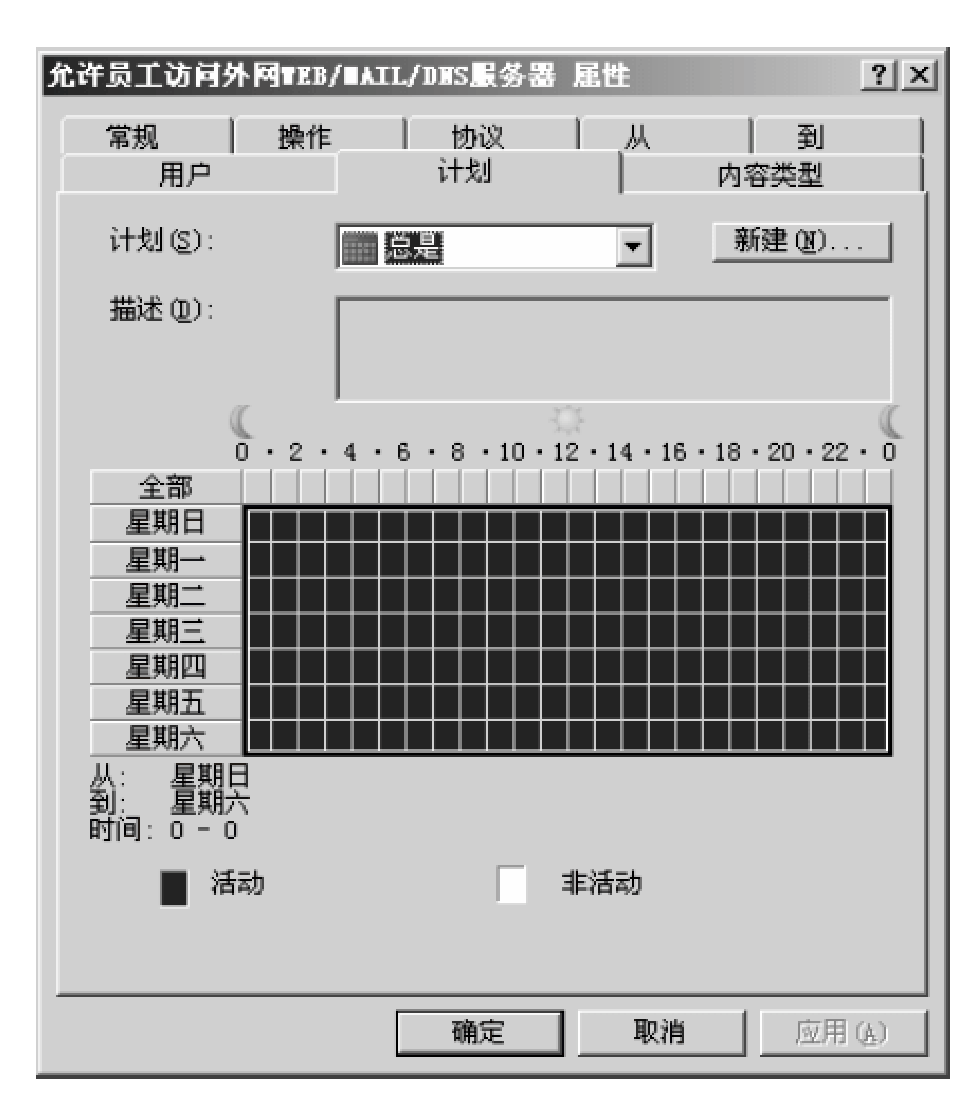


图 14-54

03 弹出【新建计划】对话框，在【名称】文本框中输入“员工上网时间”，在下侧时间区域选择不允许上网的时间段，单击【非活动】单选按钮，调整结束后，单击【确定】按钮，如图 14-55 所示。

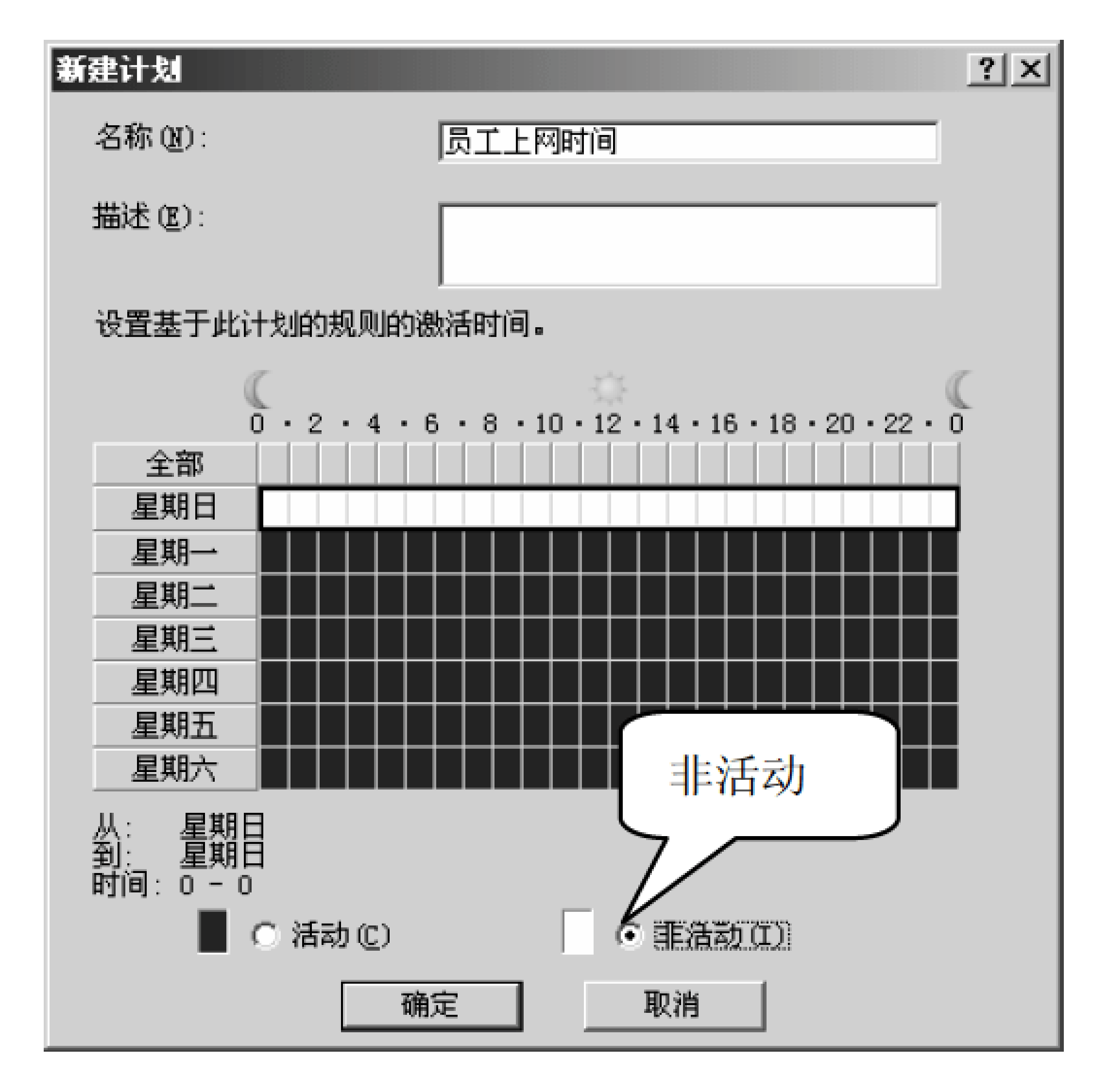


图 14-55

04 配置结束，返回属性窗口，在【计划】选项列表中使用“员工上网时间”，如图 14-56 所示，单击【确定】按钮。

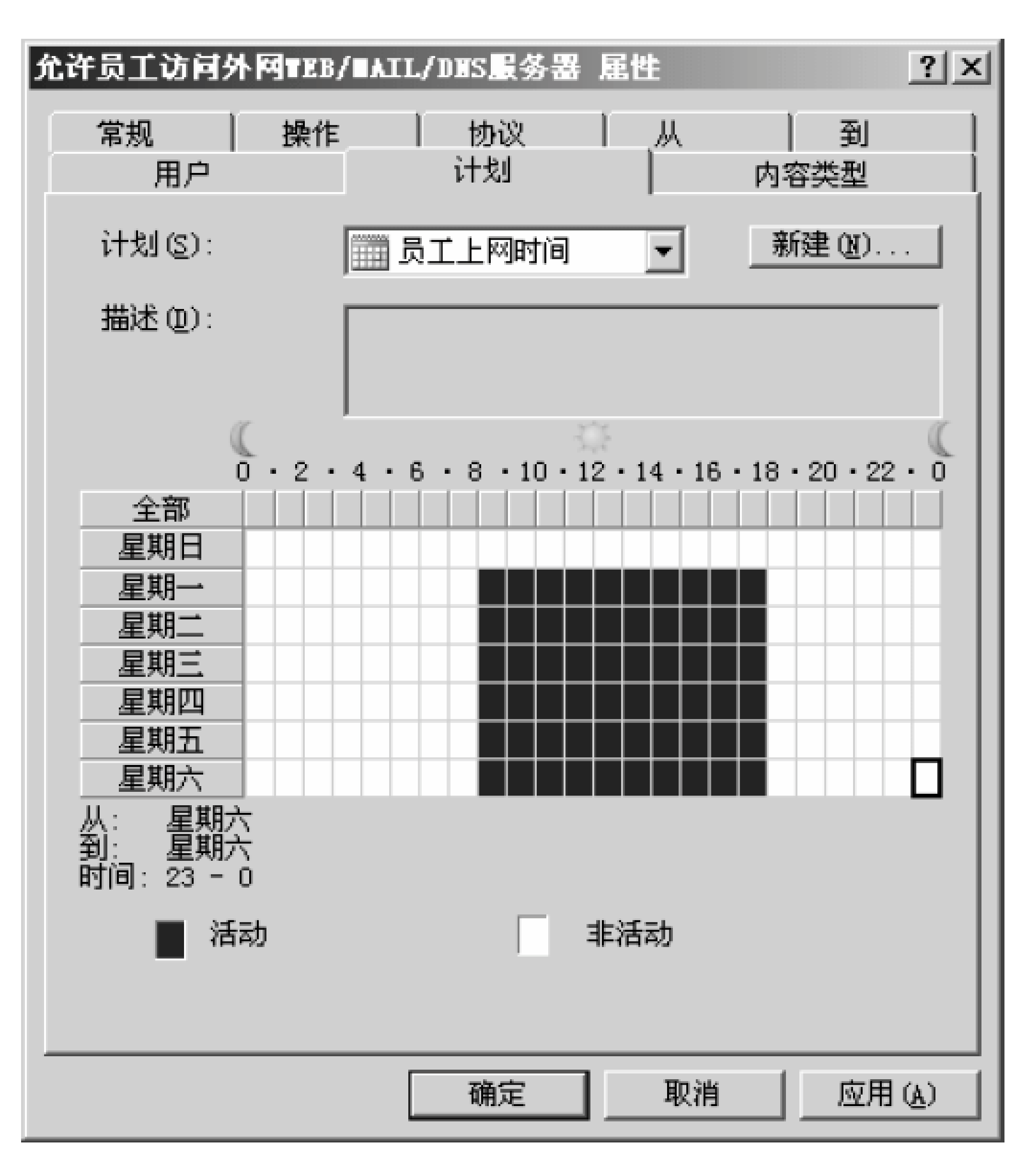


图 14-56

05 返回程序主界面，单击【应用】按钮，使配置生效，如图 14-57 所示。

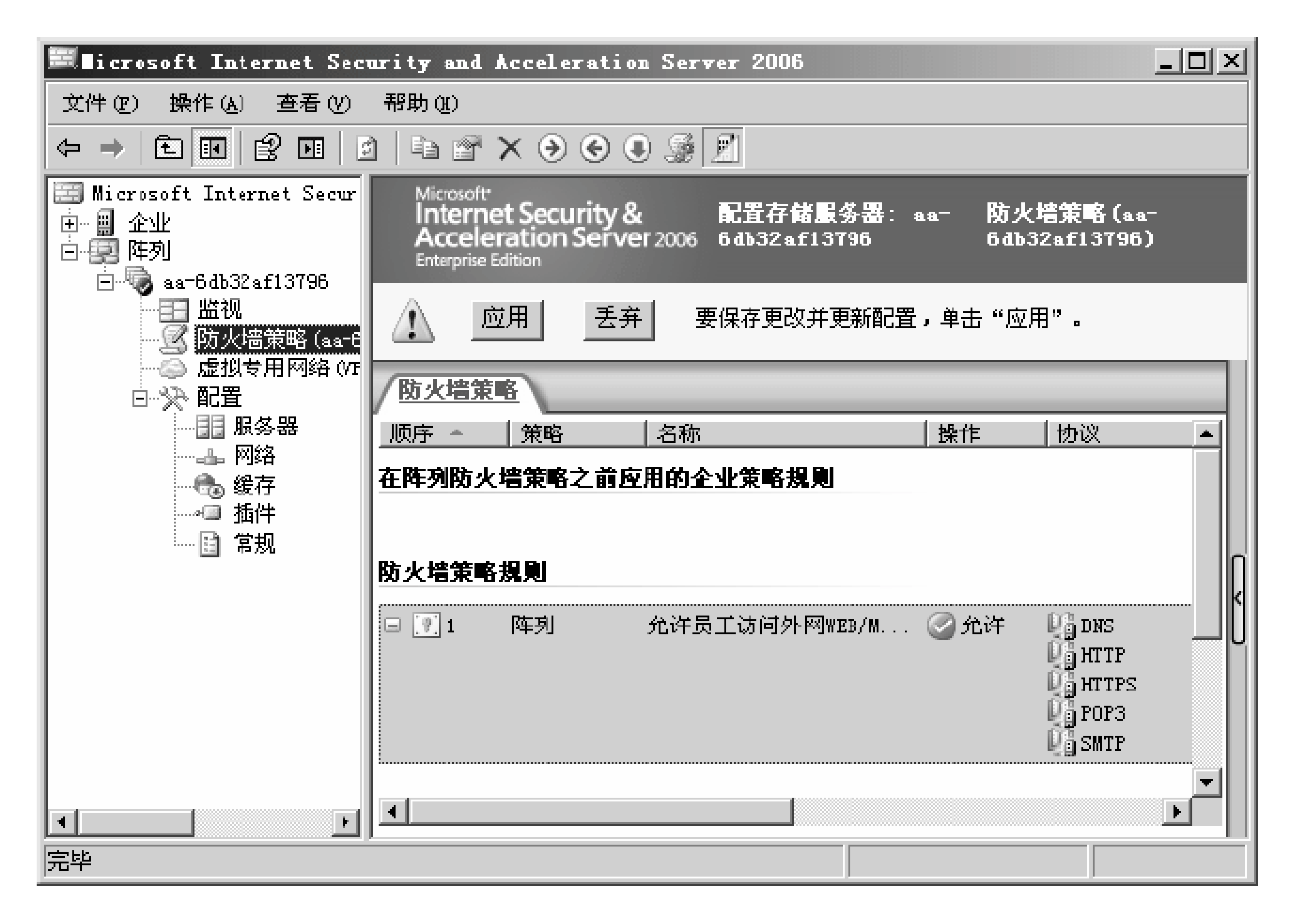


图 14-57

14.3.3 限制员工访问特殊域名网站

信息产业飞速发展，各类娱乐网站层出不穷，像 QQ 空间、开心网、迅雷看看等。很多员工沉迷于这些网站，比如前几年的“偷菜”热，“偷菜”几乎成了人们生活、工作中的一部分，这让很多领导烦恼不已。对此，ISA 防火墙可以做出针对性的限制，具体操作步骤如下。

01 打开【新建访问规则向导】对话框，在【访问规则名称】文本框中输入“不允许员工访问 QQ 空间等娱乐网站”，如图 14-58 所示，单击【下一步】按钮。

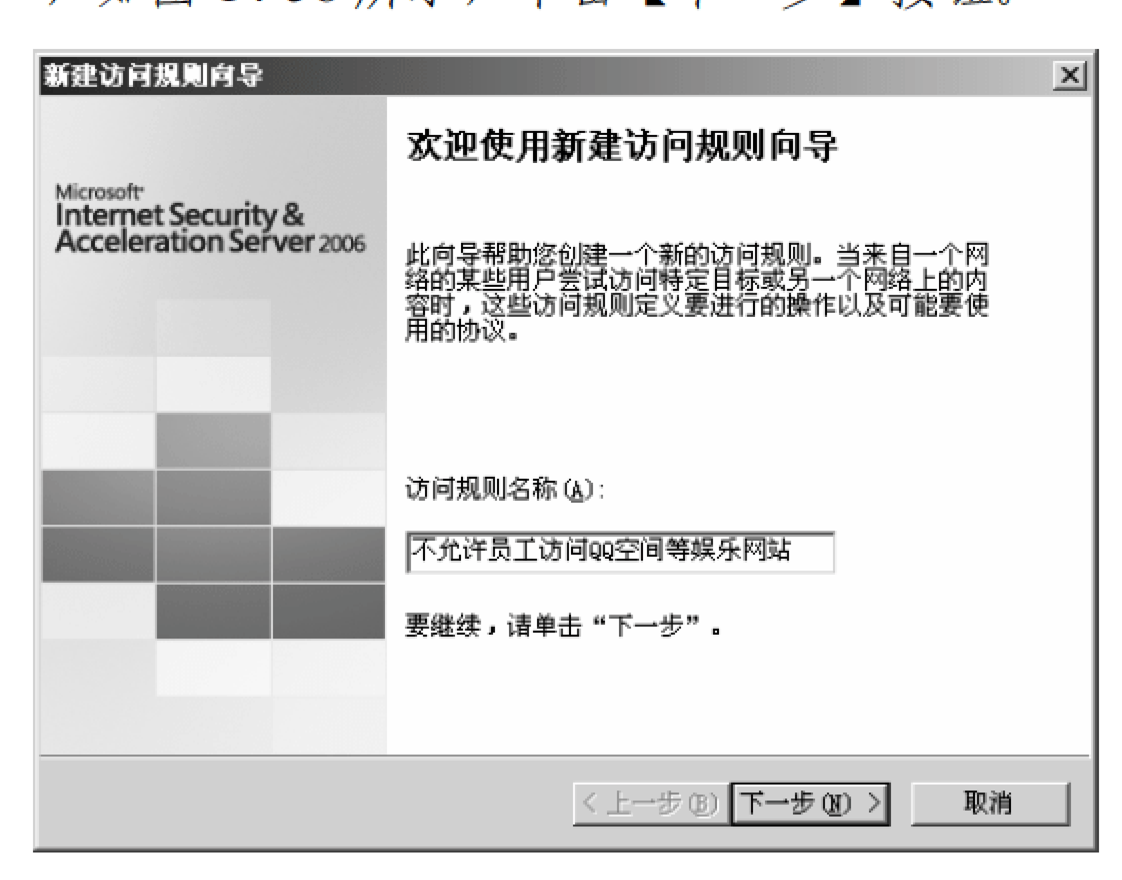


图 14-58

02 弹出【规则操作】对话框，选择【拒绝】单选按钮，单击【下一步】按钮，如图 14-59 所示。

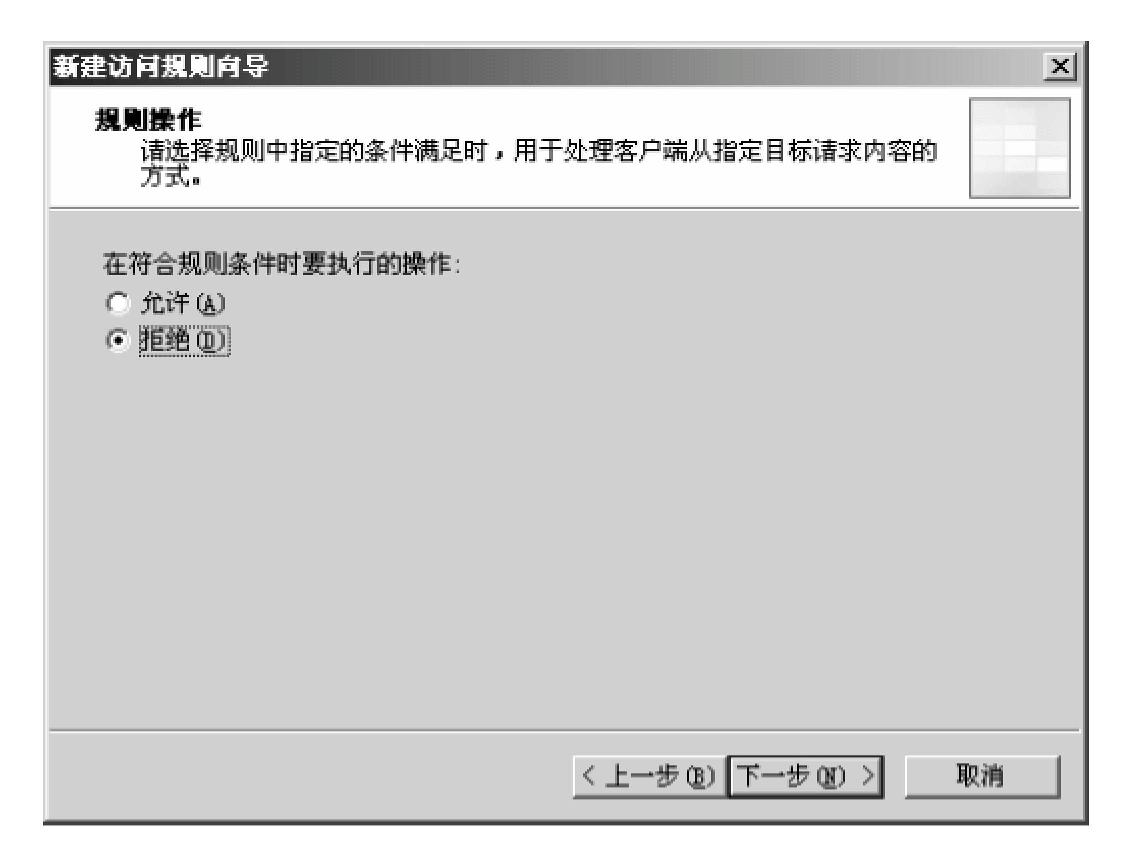


图 14-59

03 弹出【协议】对话框，通过【添加】按钮，将 DNS/HTTP/HTTPS 等协议加入列表，如图 14-60 所示，单击【下一步】按钮。



图 14-60

04 弹出【访问规则源】对话框，将【内部】网络加入列表中，如图 14-61 所示，单击【下一步】按钮。



图 14-61

05 弹出【访问规则目标】对话框，单击【添加】按钮，弹出【添加网络实体】对话框，如

图 14-62 所示，在【网络实体】列表中选择【新建】➢【URL 集】菜单命令。



图 14-62

06 弹出【新建 URL 集规则元素】对话框，在【名称】文本框中输入“员工不可访问网站”，如图 14-63 所示，单击【添加】按钮可在图中添加具有匹配特征的网址。

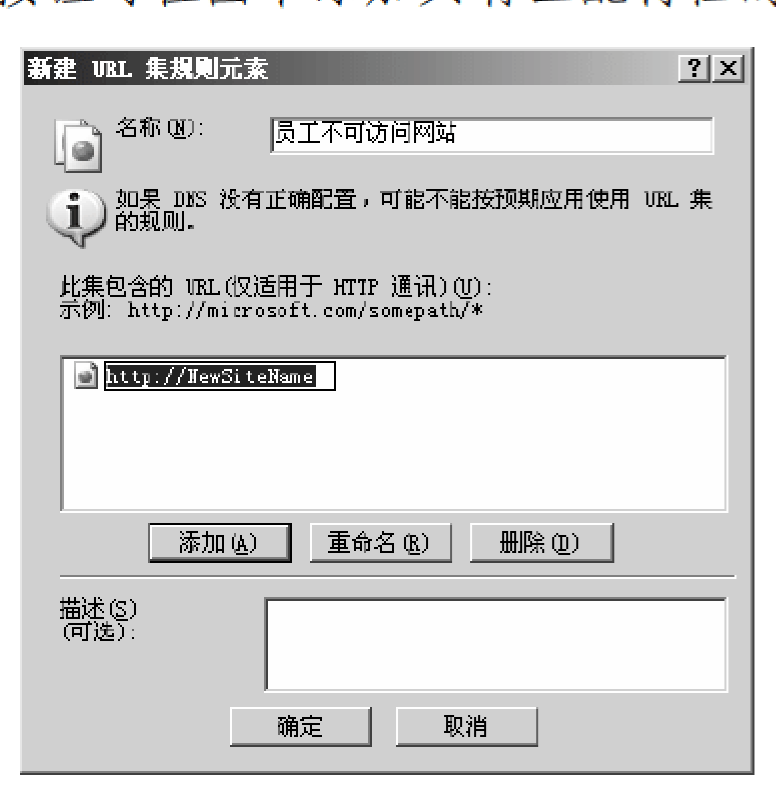


图 14-63

07 员工不可访问网址添加完成，其中“*”号代表匹配任意字符串，如图 14-64 所示，单击【确定】按钮。

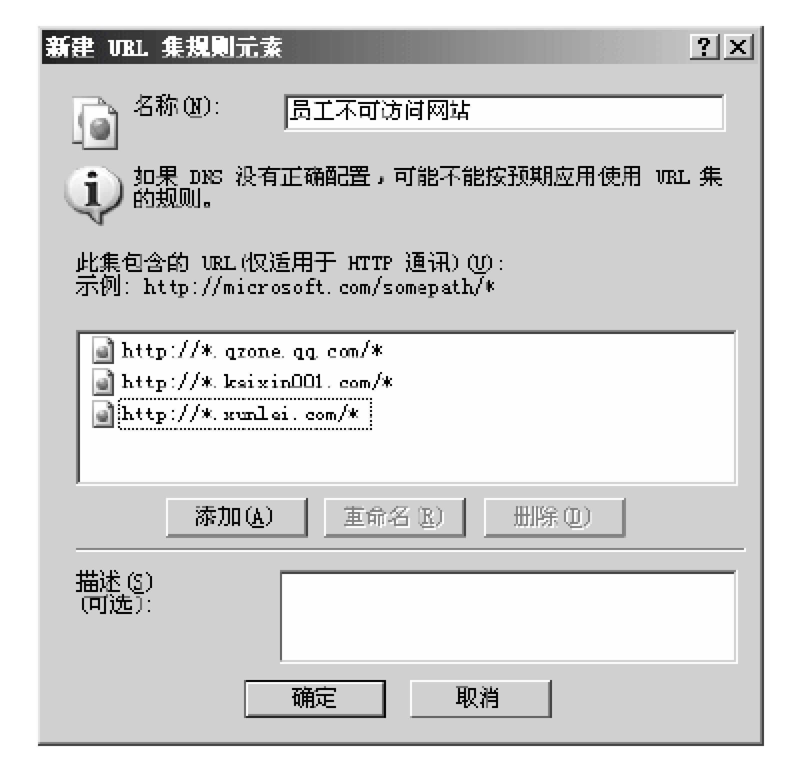


图 14-64

08 返回【访问规则目标】对话框，不可访问目标网站添加成功，如图 14-65 所示，单击【下一步】按钮。

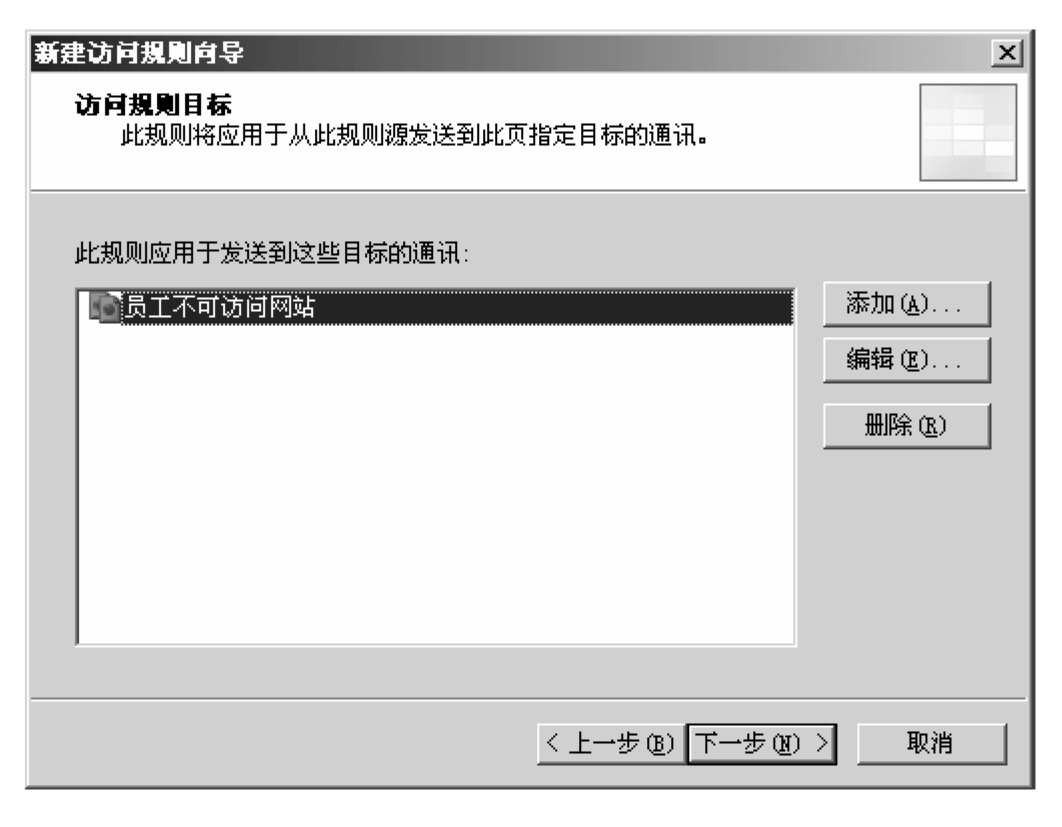


图 14-65

09 弹出【用户集】对话框，默认将该规则应用到所有用户的请求，如图 14-66 所示，单击【下一步】按钮。

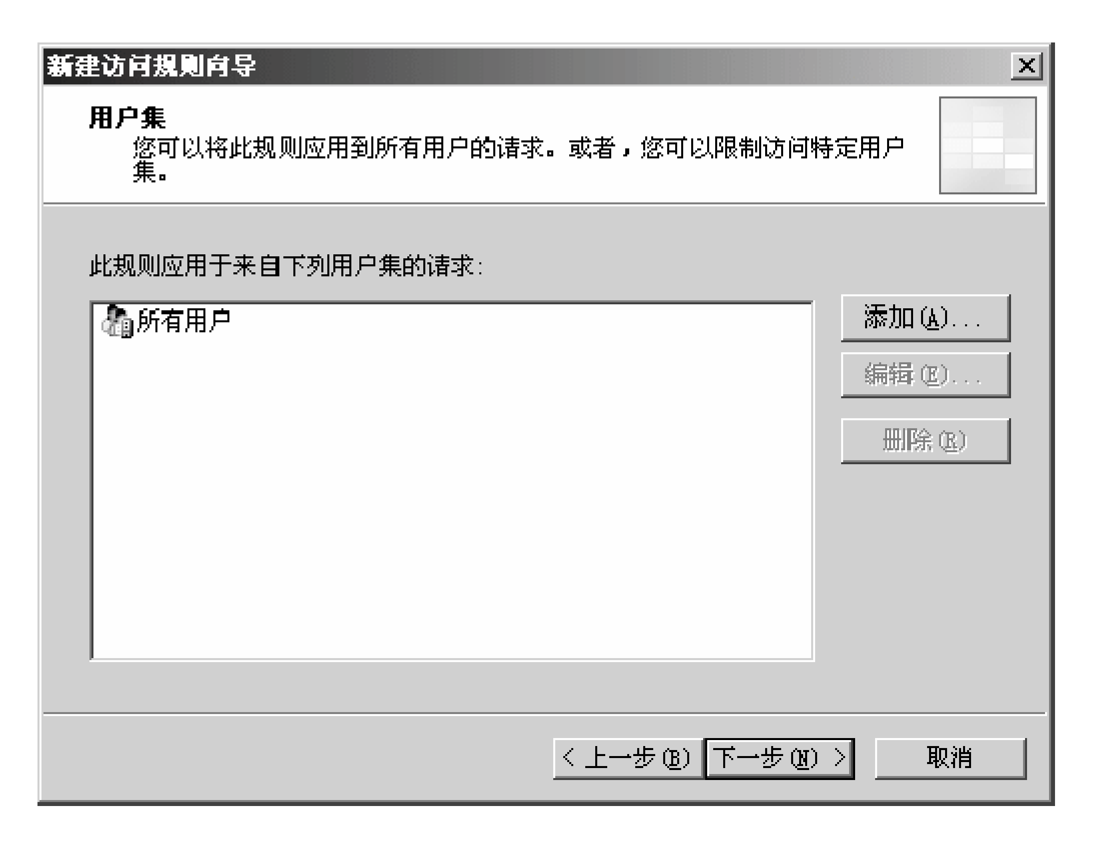


图 14-66

10 配置完成，在弹出的对话框中显示了配置信息摘要，如图 14-67 所示，单击【完成】按钮，并在程序主界面应用该配置。

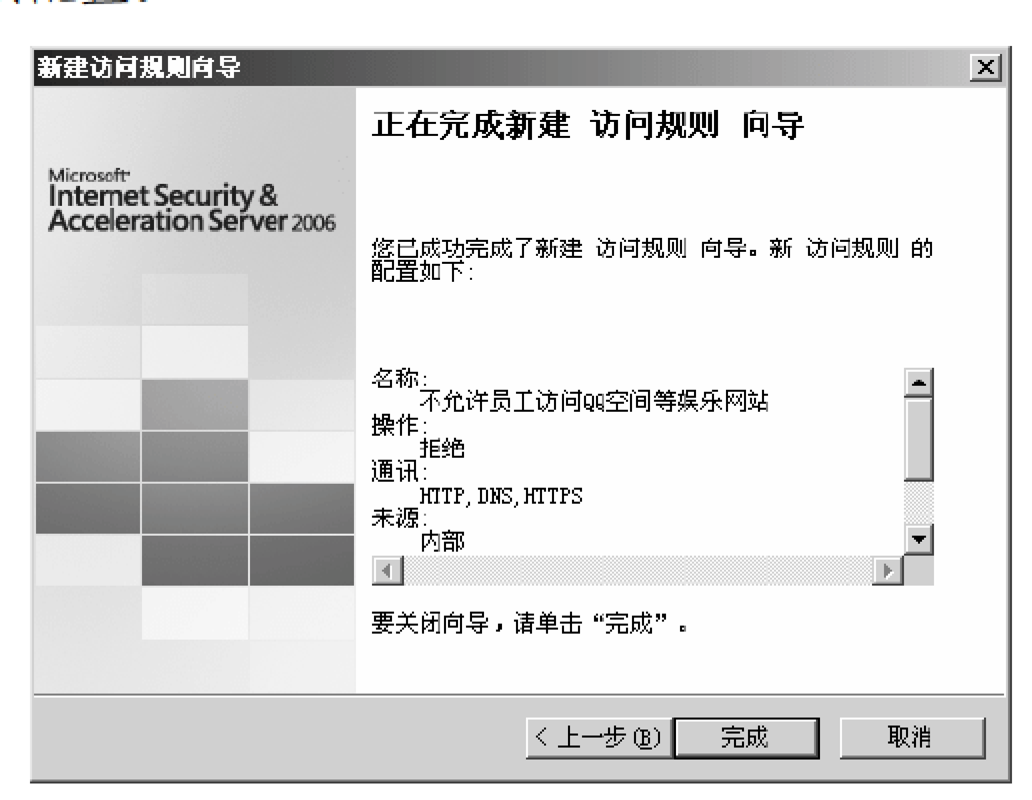


图 14-67

14.3.4 限制员工使用迅雷等下载工具

企业的网络带宽资源一般都很有限，特别是中小企业。有限的资源如果被恶意占用，会严重影响公司业务的运行。其中影响最大的就是在线视频、网络下载。在线视频可以通过 14.3.3 节内容进行域名限制，下面主要介绍网络下载的限制方法。

1. 限制 HTTP 下载

很多浏览器自带下载功能，通常情况下这部分网络下载流量会被网络管理员忽略，但是如果放任不管的话，依然会造成很大比例的网络资源浪费。

限制 HTTP 下载的具体操作步骤如下。

01 右击允许员工访问互联网的防火墙策略，在弹出的快捷菜单中选择【配置 HTTP】菜单命令，如图 14-68 所示。



图 14-68

02 弹出【为规则配置 HTTP 策略】对话框，选择【扩展名】选项卡，在【指定对文件扩展名要执行的操作】选项列表中选择【阻止指定的扩展名（允许所有其他扩展名）】选项，单击【添加】按钮，如图 14-69 所示。

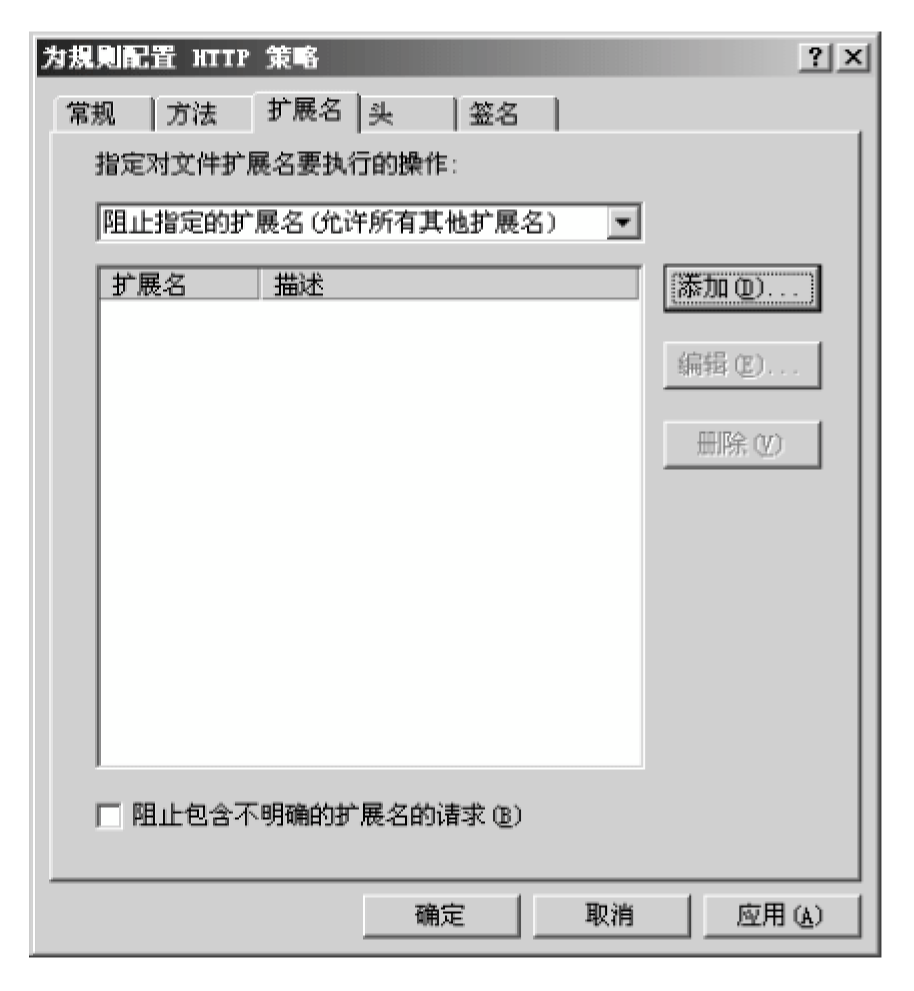


图 14-69

03 弹出【扩展名】对话框，在【扩展名】文本框中输入可能被下载的文件后缀，如图 14-70 所示，一般视频媒体文件被定为禁止下载内容，单击【确定】按钮，完成添加。



图 14-70

04 按照 14.3.3 小节步骤添加被限制下载的所有文件类型，添加结果如图 14-71 所示，选择【阻止包含不明确的扩展名的请求】复选框，单击【确定】按钮。

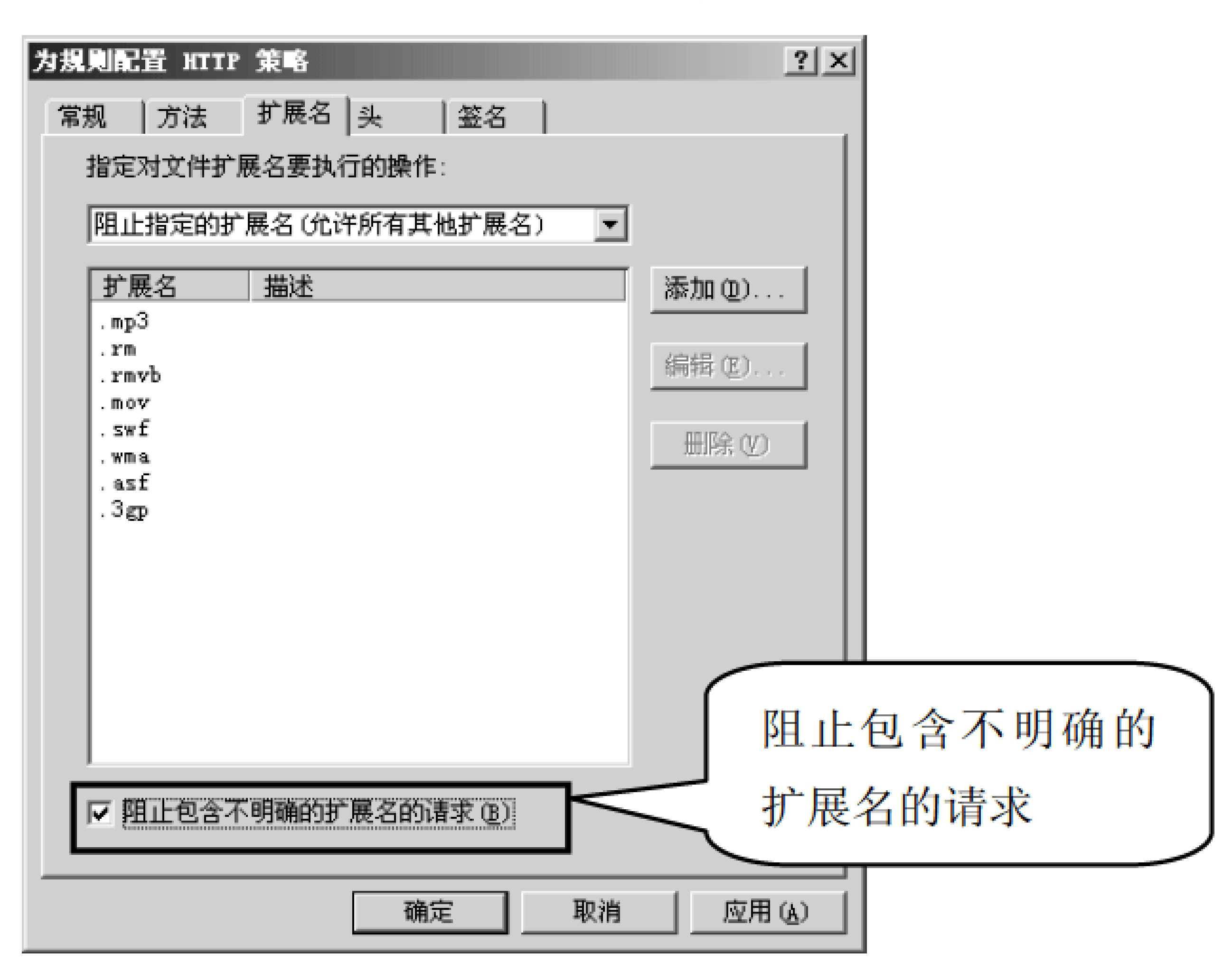


图 14-71

05 返回程序主界面，单击【应用】按钮使配置生效，如图 14-72 所示。

图 14-72

2. 限制迅雷及 BT

一般限制迅雷操作比较难，可以使用“限制 HTTP 下载”的方式。如果想彻底封锁迅雷可以通过网络搜索所有迅雷的服务器 IP 地址，将这些地址封掉就可以了，但是迅雷的服务器 IP 地址比较多，操作起来会有些麻烦。

BT 流量的封锁也可以使用“限制 HTTP 下载”的方式。同时还可以使用签名的方式封锁 BT。当 BT 客户端下载时，在 HTTP 请求的数据包中，包含了带有 BT 特征的特殊字符串头(User-Agent): BitTorrent。所以，可以据此使用签名的方式将 BT 流量封掉。详细操作步骤如下。

01 右击允许员工访问互联网的防火墙策略，选择【配置 HTTP】菜单命令，弹出【为规则配置 HTTP 策略】对话框。如图 14-73 所示，选择【签名】选项卡，单击【添加】按钮。



图 14-73

02 弹出【签名】对话框，在【名称】对话框输入本条签名名称“BT 流量”，在【查找范围】文本框的下拉选项中选择【请求头】选项，在【HTTP 头】文本框中输入“User-Agent”，在【签名】文本框中输入“BitTorrent”，如图 14-74 所示，单击【确定】按钮。



图 14-74

03 返回程序主界面，单击【应用】按钮使配置生效，如图 14-75 所示。



图 14-75

14.4　项目实施 3：利用 ISA 发布企业内网服务器

在 DMZ 区放置了企业对外发布服务器，主要有 WEB 服务器、DNS 服务器、E-Mail 服务器等。下面详细介绍这些服务器的发布。

14.4.1 ISA 防火墙安全发布 WEB 服务器

WEB 服务器是企业最重要的对外发布服务器之一，大部分企业都会用到。

单一 WEB 服务器的发布操作步骤。

01 在左侧列表选择【防火墙策略】选项，在右侧窗格选择【任务】选项卡，单击【发布网站】选项，如图 14-76 所示。



图 14-76

02 弹出【新建 Web 发布规则向导】对话框，在【Web 发布规则名称】文本框中输入“DMZ 区对外发布 WEB 服务器”，如图 14-77 所示，单击【下一步】按钮。

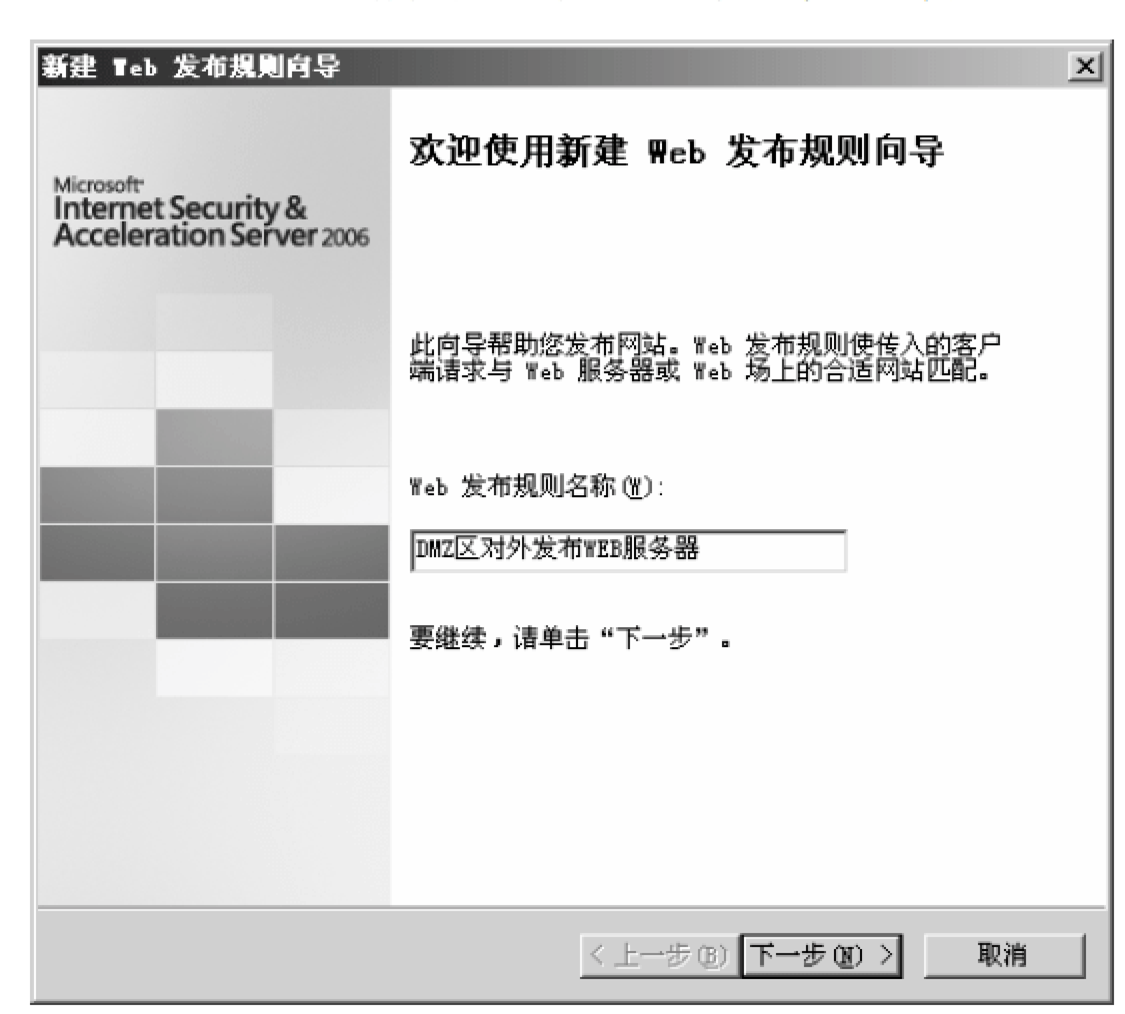


图 14-77

03 弹出【请选择规则操作】对话框，选择【允许】单选按钮，如图 14-78 所示，单击【下一步】按钮。

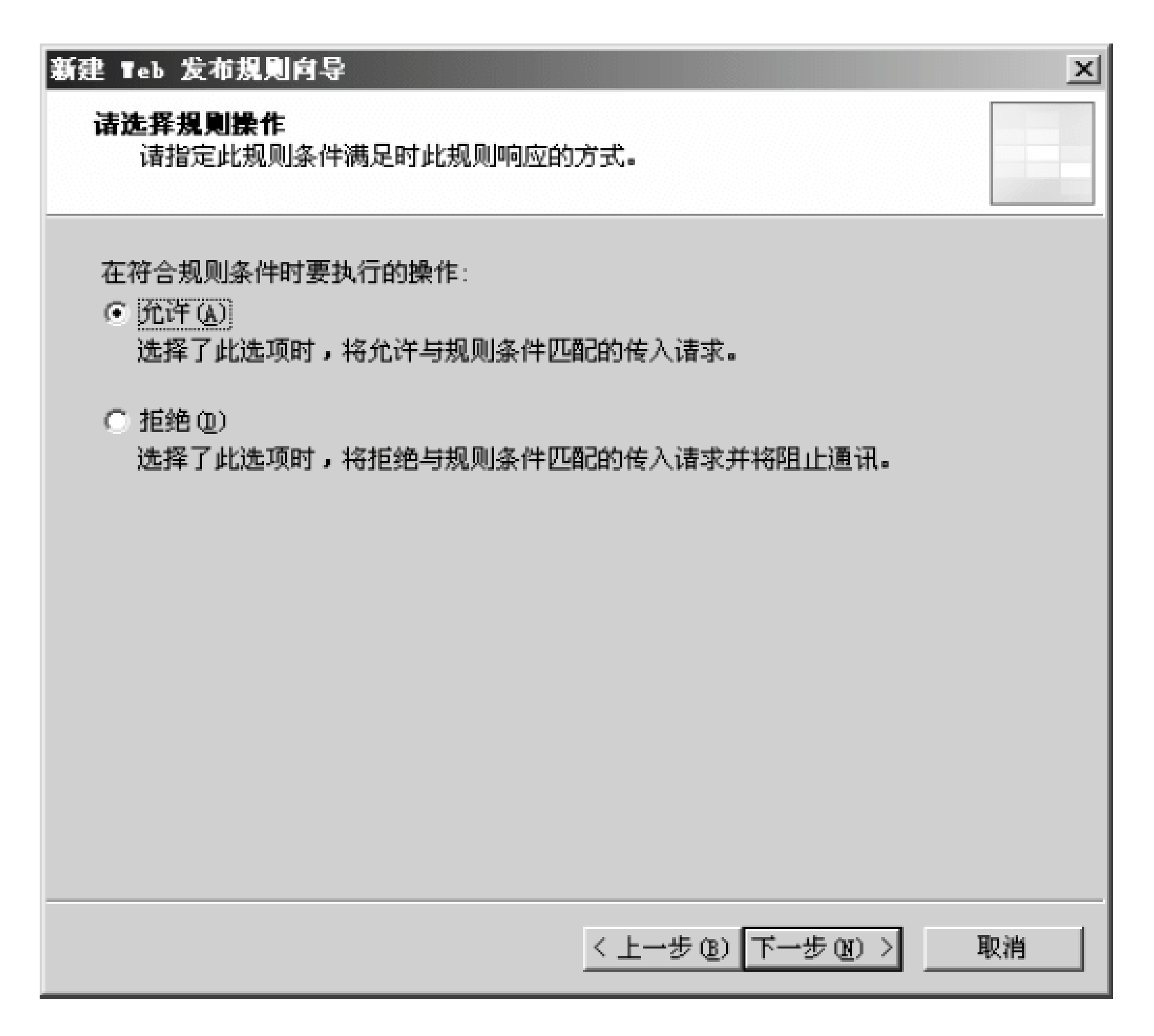


图 14-78

04 弹出【发布类型】对话框，选择【发布单个网站或负载平衡器】单选按钮，如图 14-79 所示，单击【下一步】按钮。

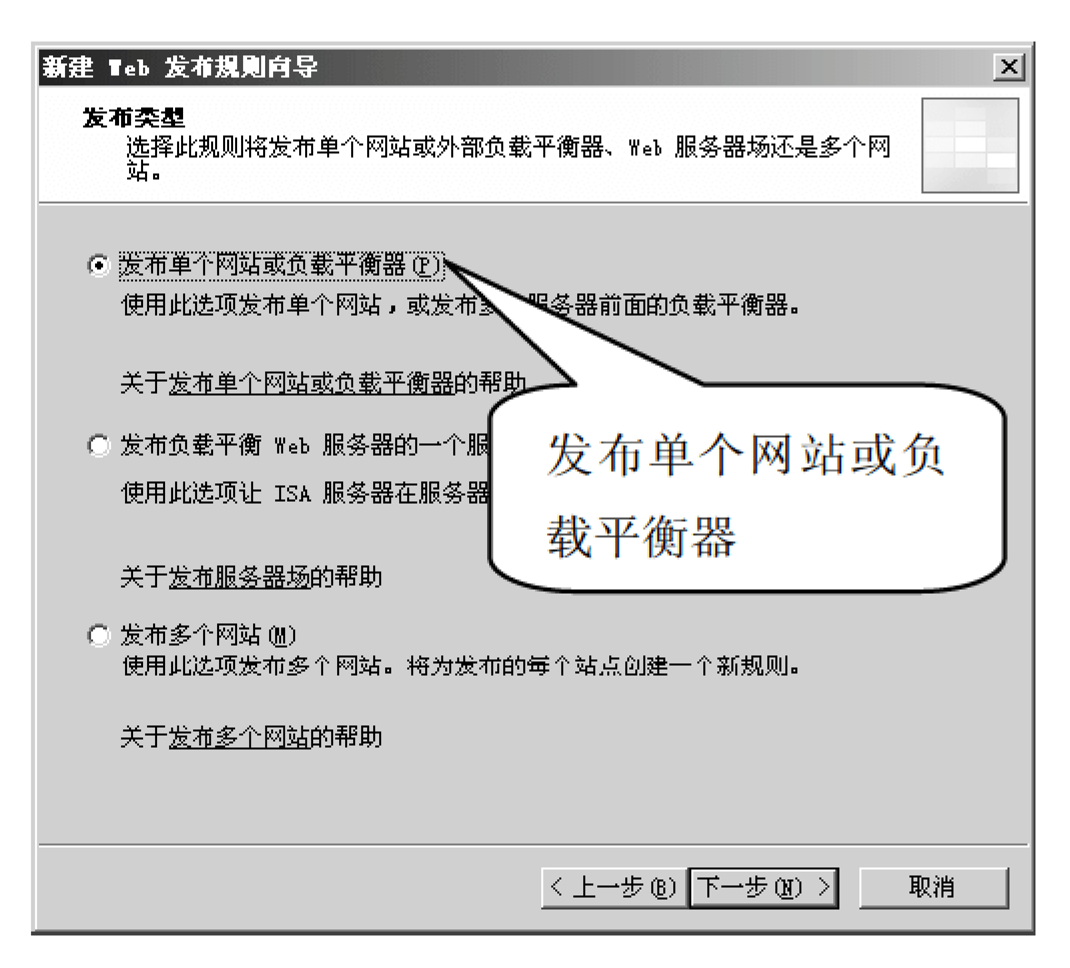


图 14-79

05 弹出【服务器连接安全】对话框，选择【使用不安全的连接连接发布的 Web 服务器或服务器场】单选按钮，如图 14-80 所示。



图 14-80



提　示

如果使用 SSL 连接发布服务器，必须要有认证系统，否则网站发布会失败，本实例不做 SSL 连接。

06 弹出【内部发布详细信息】对话框，在【内部站点名称】文本框中输入网站在内网使用的域名，本实例采用“www.web.com”，为了内网服务器可以被访问到，在【计算机名称或 IP 地址】文本框中输入 DMZ 区 Web 服务器的 IP 地址“192.168.100.100”，如图 14-81 所示，单击【下一步】按钮。



图 14-81

07 在弹出的对话框中，选择默认配置，单击【下一步】按钮，如图 14-82 所示。

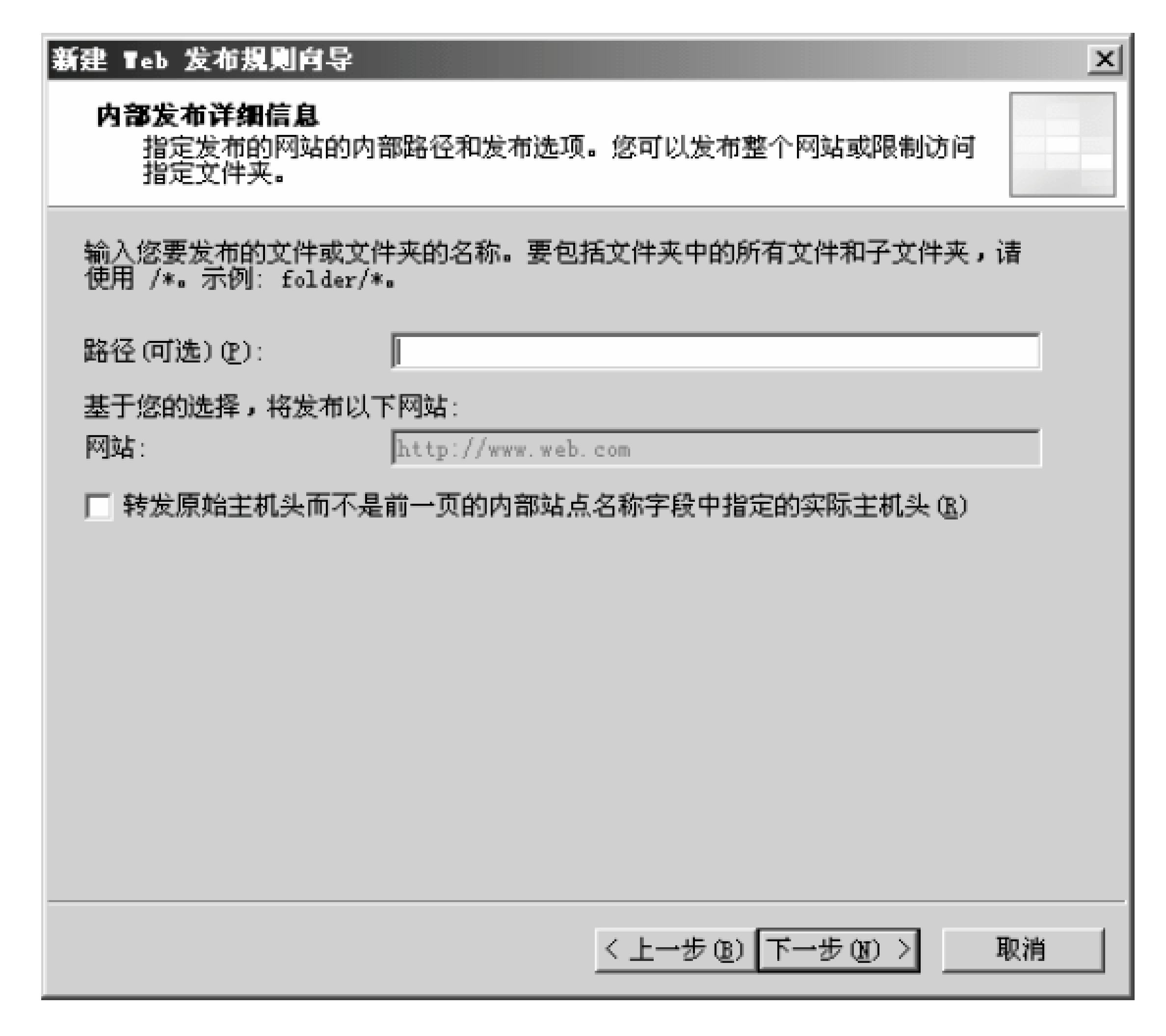


图 14-82

08 弹出【公共名称细节】对话框，在【公用名称】文本框中输入公网访问企业网站使用的域名，该域名需要在域名注册机构注册，本实例使用“www.web.com”为例讲解，如图 14-83 所示，单击【下一步】按钮。



图 14-83

09 弹出【选择 Web 侦听器】对话框，单击【新建】按钮，如图 14-84 所示。



图 14-84

10 弹出【新建 Web 侦听器定义向导】对话框，在【Web 侦听器名称】文本框中输入“外部WEB 访问”，如图 14-85 所示，单击【下一步】按钮。

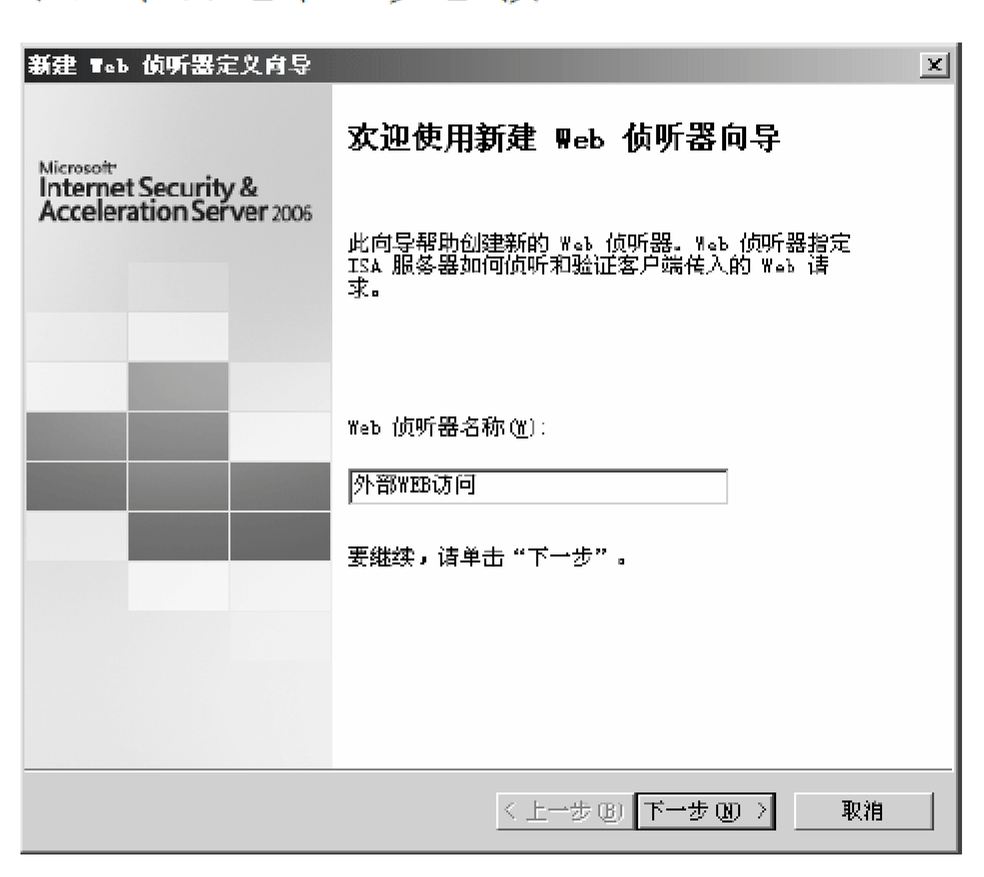


图 14-85

11 弹出【客户端连接安全设置】对话框，由于本实例不采用 SSL 安全连接，所以选择【不需要与客户端建立 SSL 安全连接】单选按钮，如图 14-86 所示，单击【下一步】按钮。

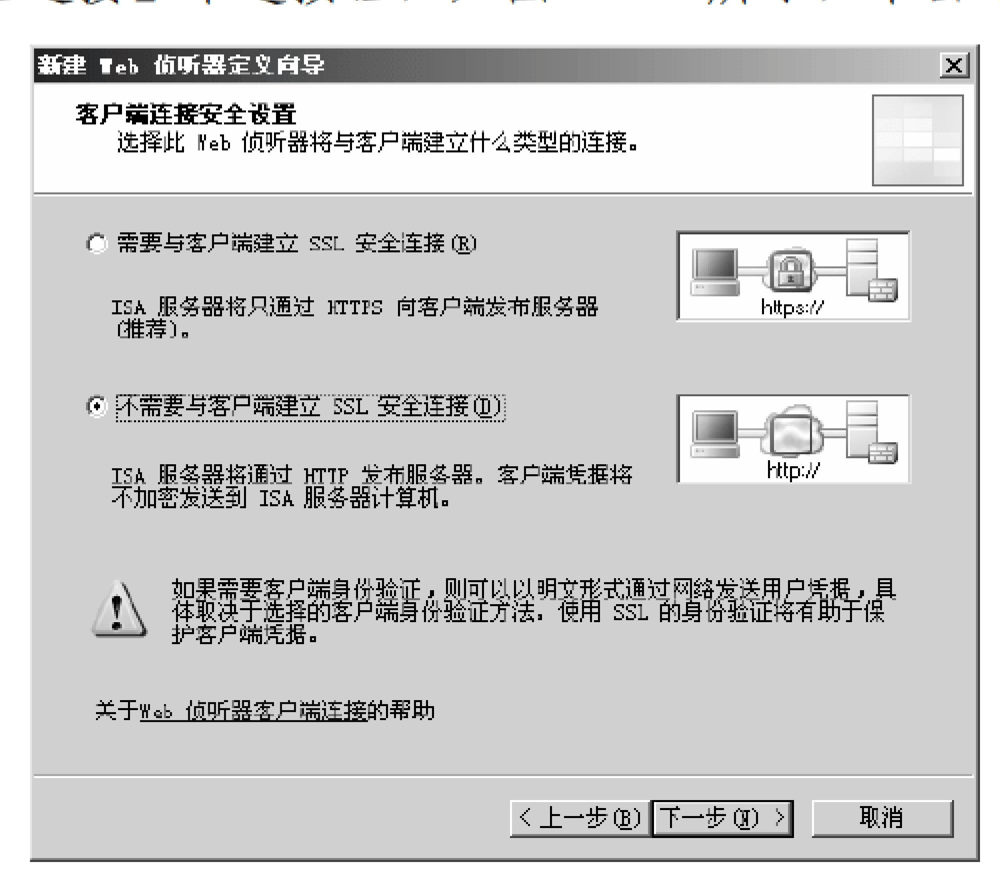


图 14-86

12 弹出【Web 侦听器 IP 地址】对话框，选择侦听 Web 访问请求的端口或地址段，选择【外部】复选框，如图 14-87 所示，单击【下一步】按钮。

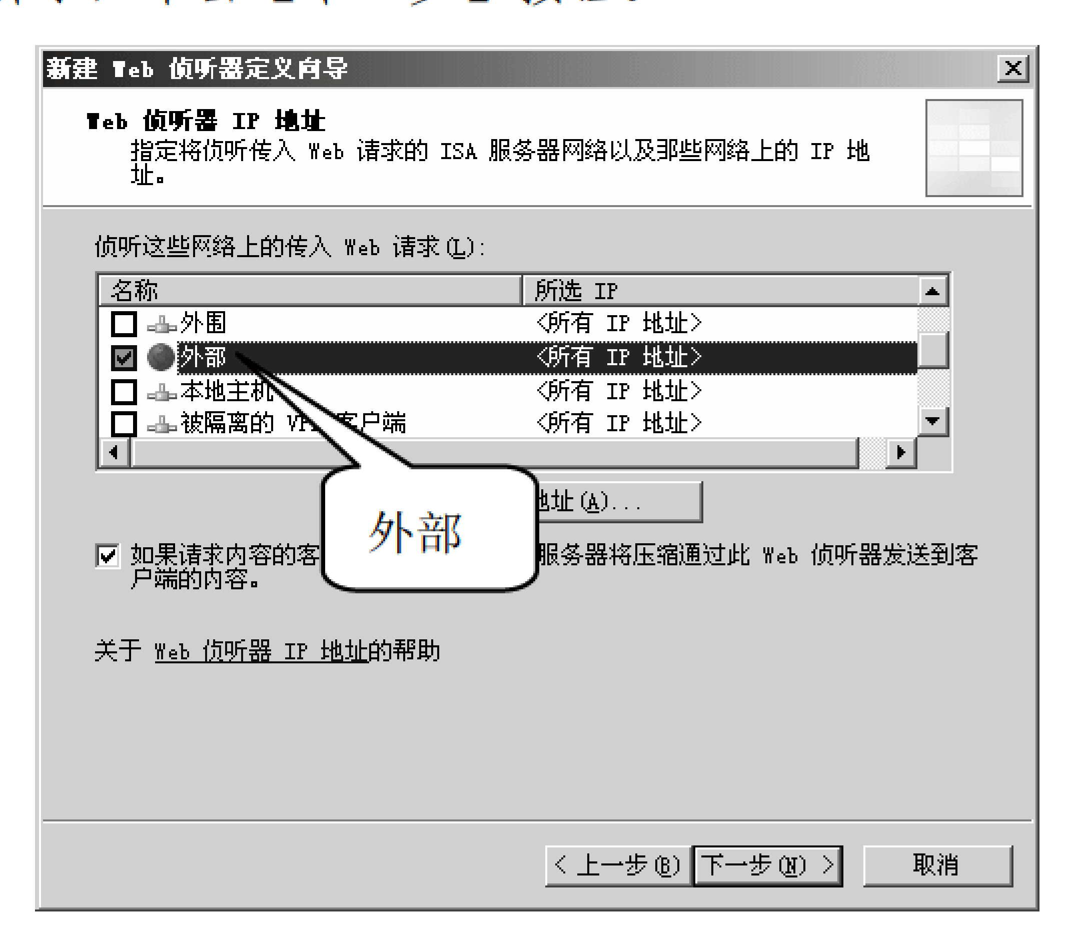


图 14-87

13 弹出【身份验证设置】对话框，选择【没有身份验证】选项，单击【下一步】按钮，如图 14-88 所示。

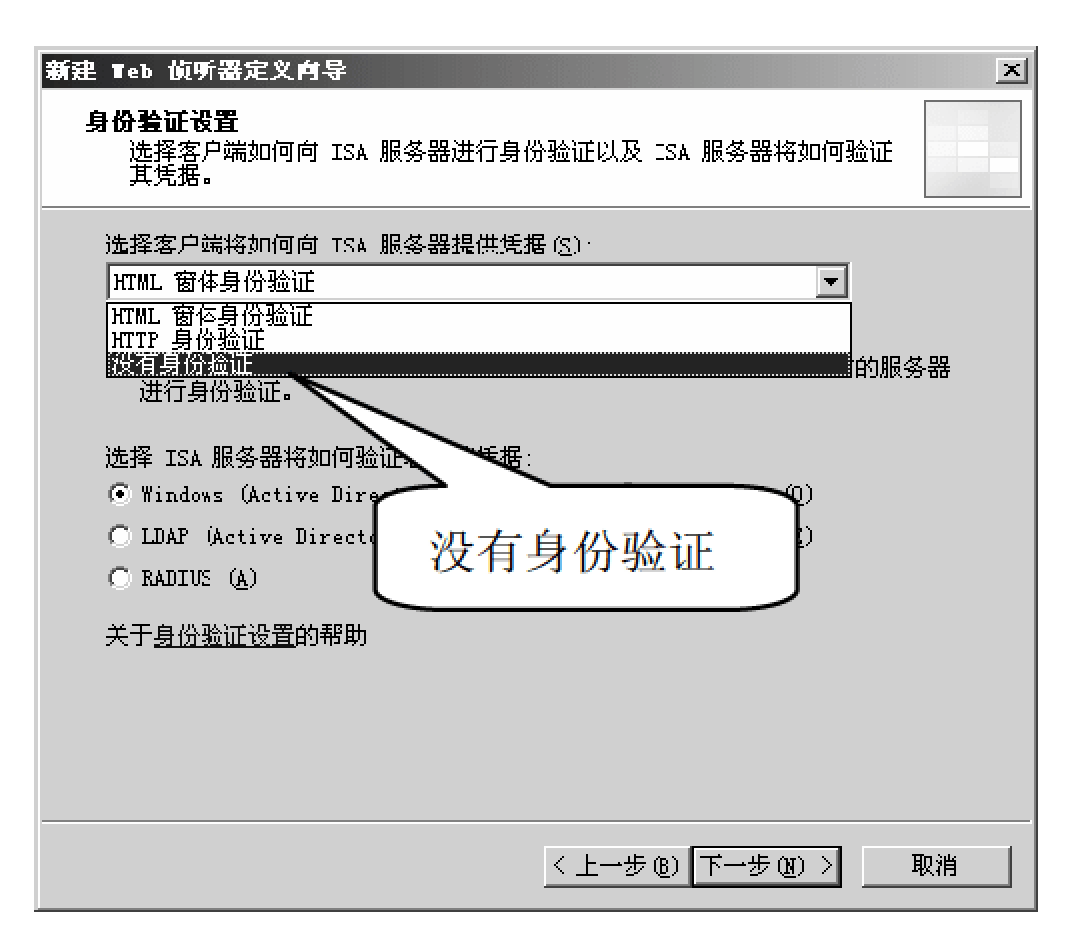


图 14-88

14 弹出【单一登录设置】对话框，本实例中没有身份认证问题，不做操作，如图 14-89 所示，单击【下一步】按钮。



图 14-89

15 Web 侦听器配置完成，在弹出的对话框中显示了详细配置内容，单击【完成】按钮，如图 14-90 所示。

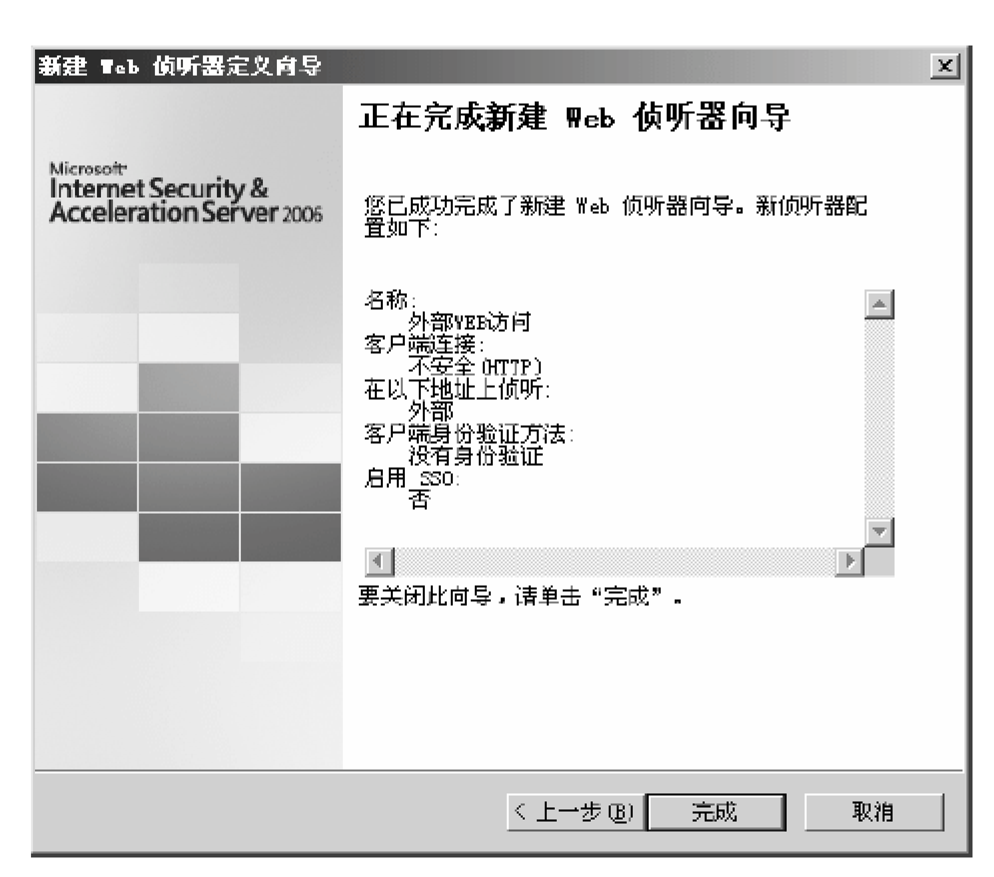


图 14-90

16 返回【选择 Web 侦听器】对话框，新建 Web 侦听器已被应用，单击【下一步】按钮，如图 14-91 所示。

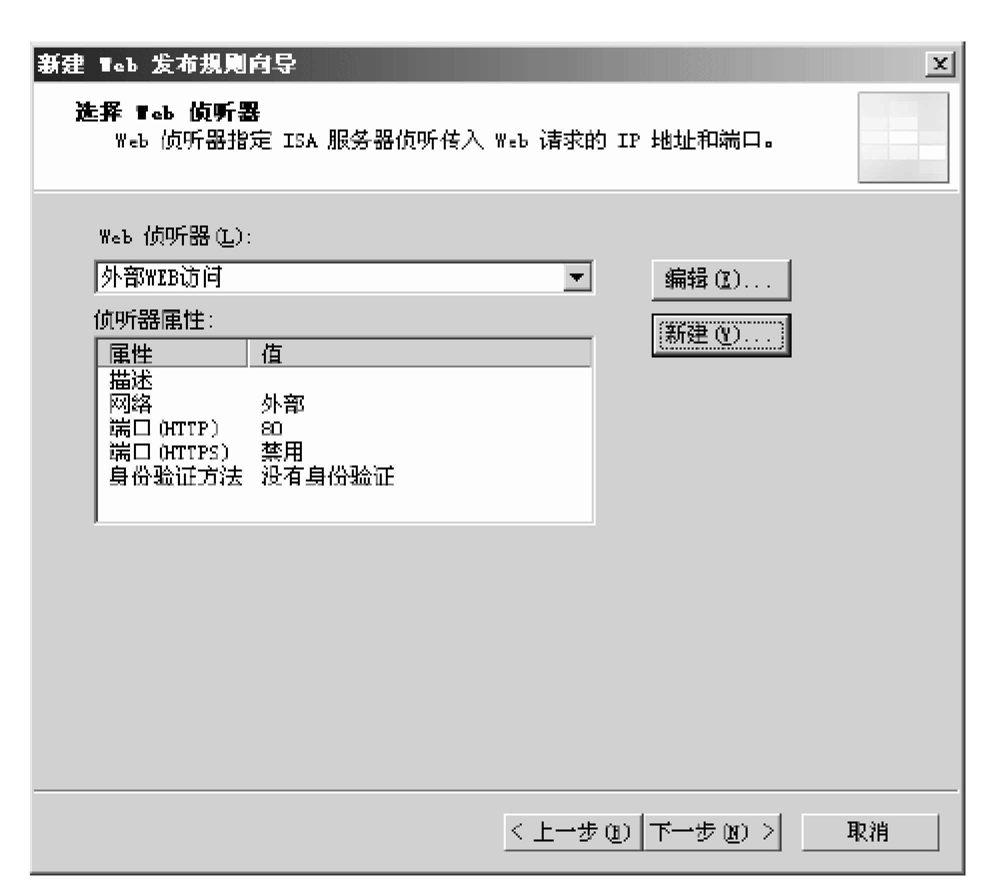


图 14-91

17 弹出【身份验证委派】对话框，因为本实例不配置身份验证，所以选择【无委派，客户端无法直接尽心身份验证】选项，如图 14-92 所示，单击【下一步】按钮。

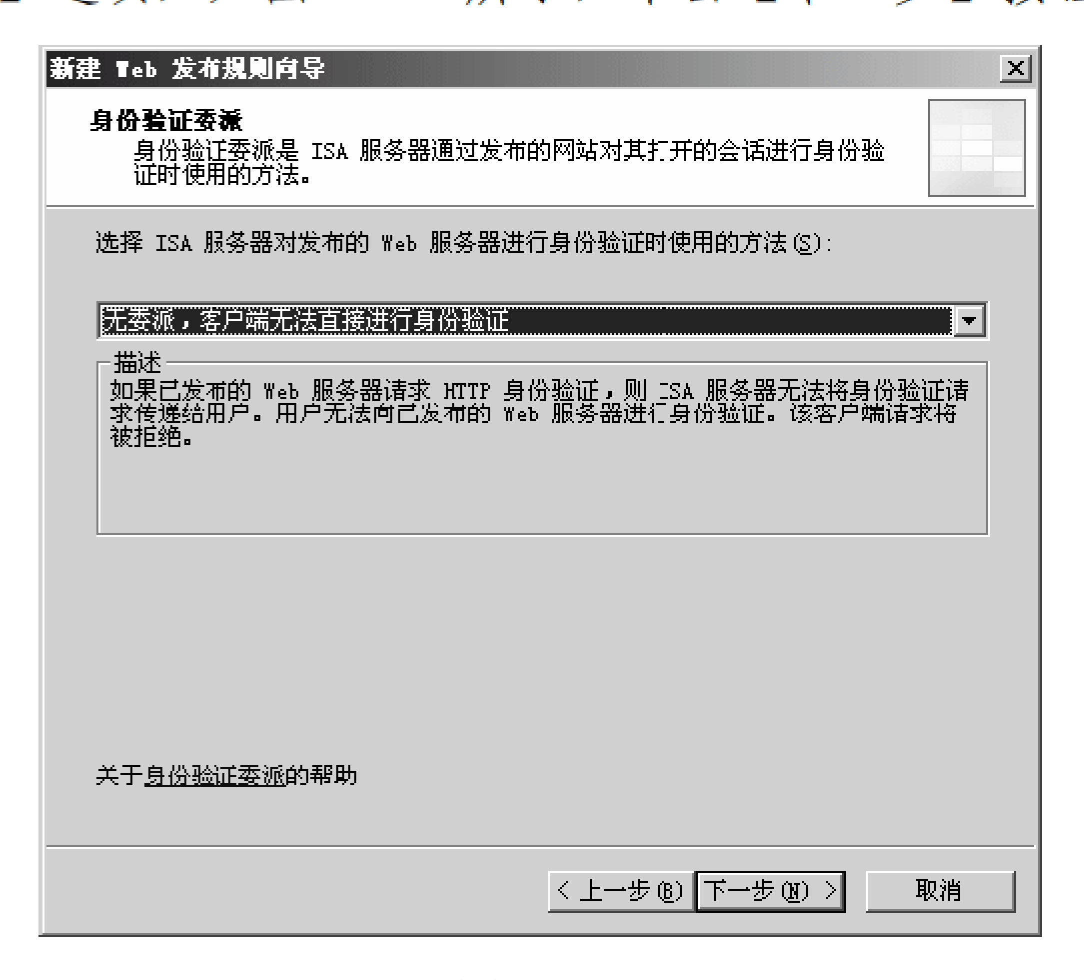


图 14-92

18 弹出【用户集】对话框，默认将此规则应用到所有用户的请求，如图 14-93 所示，单击【下一步】按钮。

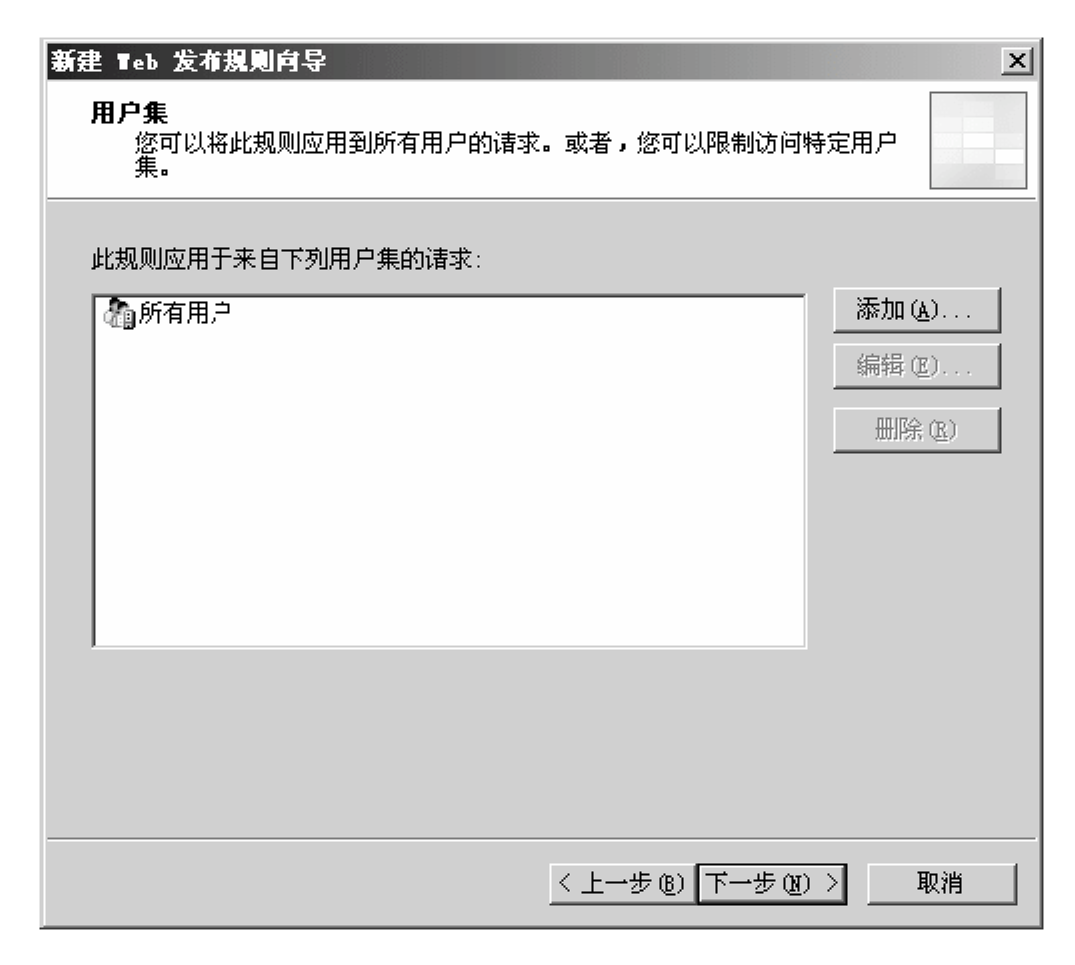


图 14-93

19 Web 服务器发布配置完成，在弹出的对话框中显示了详细的配置信息，如图 14-94 所示，单击【完成】按钮。

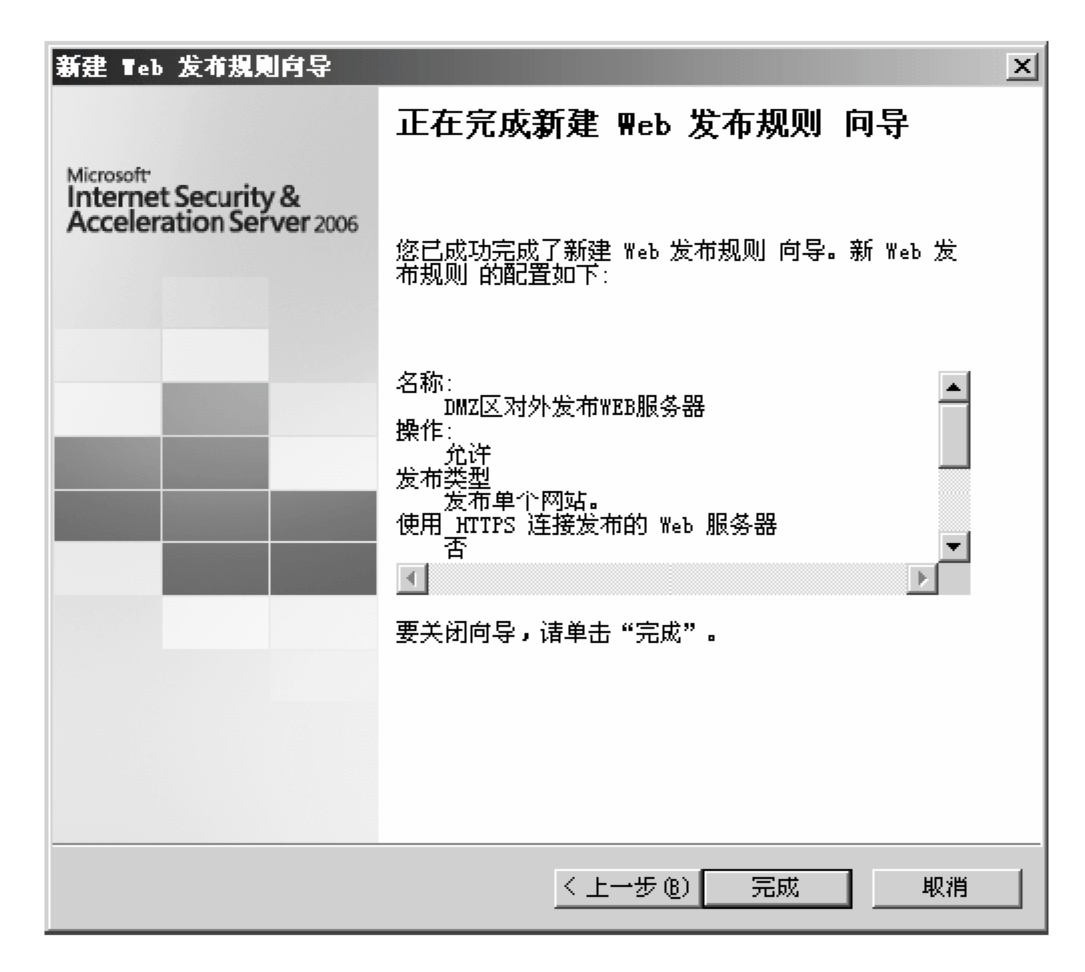


图 14-94

20 返回程序主界面，单击【应用】按钮使配置生效，如图 14-95 所示。



图 14-95



配置发布 Web 服务器时，内网和外网访问使用的域名必须是可以被 DNS 服务器解析到的。

14.4.2　ISA 防火墙安全发布邮件服务器

很多企业为了工作方便都会配备企业邮箱，为了保证企业邮箱在内外网都可以使用，这就需要防火墙发布邮件服务器。

邮件服务器的发布步骤。

01 在程序主界面右侧【任务】选项卡中，选择【发布邮件服务器】选项，如图 14-96 所示。



图 14-96

02 弹出【新建邮件服务器发布规则向导】对话框，在【邮件服务器发布规则名称】文本框中输入“企业邮件服务器”，如图 14-97 所示，单击【下一步】按钮。

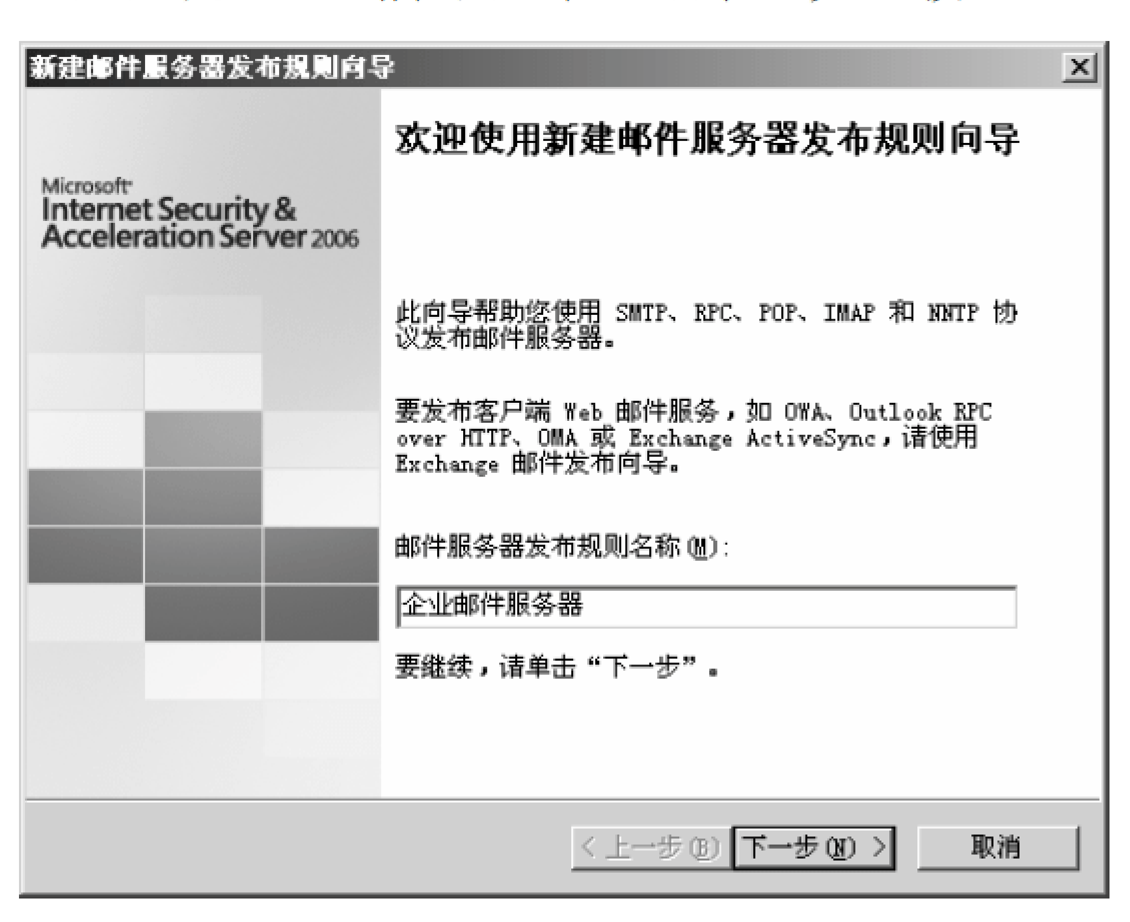


图 14-97

03 弹出【选择访问类型】对话框，选择【客户端访问：RPC、IMAP、POP3、SMTP】单选按钮，如图 14-98 所示，单击【下一步】按钮。

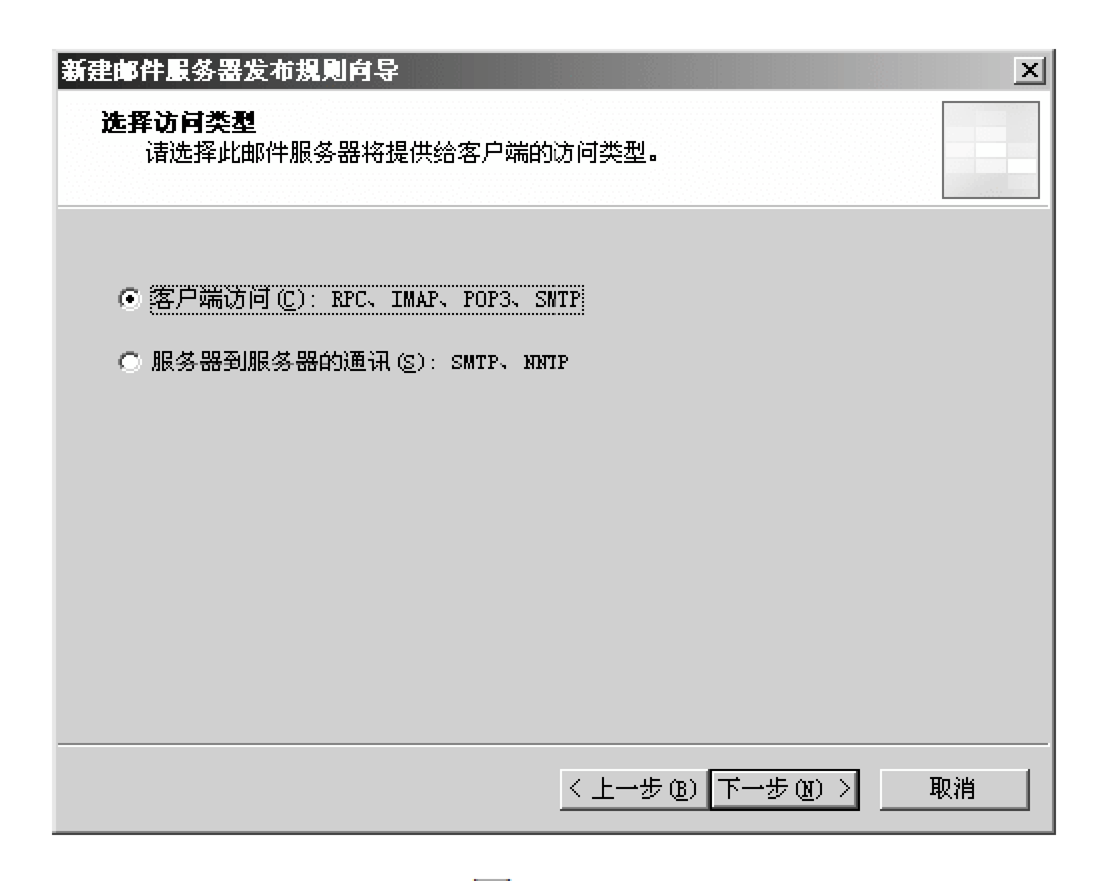


图 14-98

04 弹出【选择服务】对话框，常用邮件服务有 POP3、SMTP、IMAP4，“secure port”意思是安全端口，如果访问邮件时使用认证技术可以选择右侧三项复选框，本实例选择左侧四项复选框，如图 14-99 所示，单击【下一步】按钮。

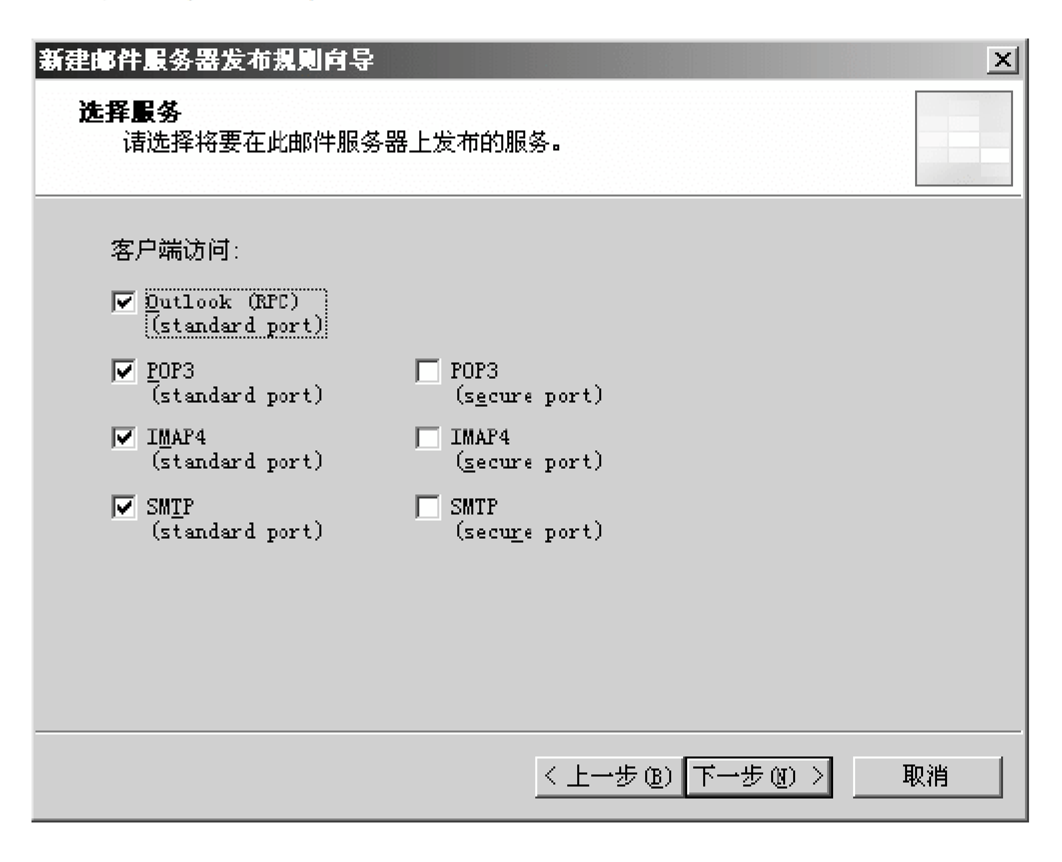


图 14-99

05 弹出【选择服务器】对话框，在【服务器 IP 地址】文本框中输入 DMZ 区邮件服务器的 IP 地址，本实例采用“192.168.100.100”地址，如图 14-100 所示，单击【下一步】按钮。

图 14-100

06 弹出【网络侦听器 IP 地址】对话框，在【侦听来自这些网络的请求】选项列表中选择【外部】复选框，如图 14-101 所示，单击【下一步】按钮。

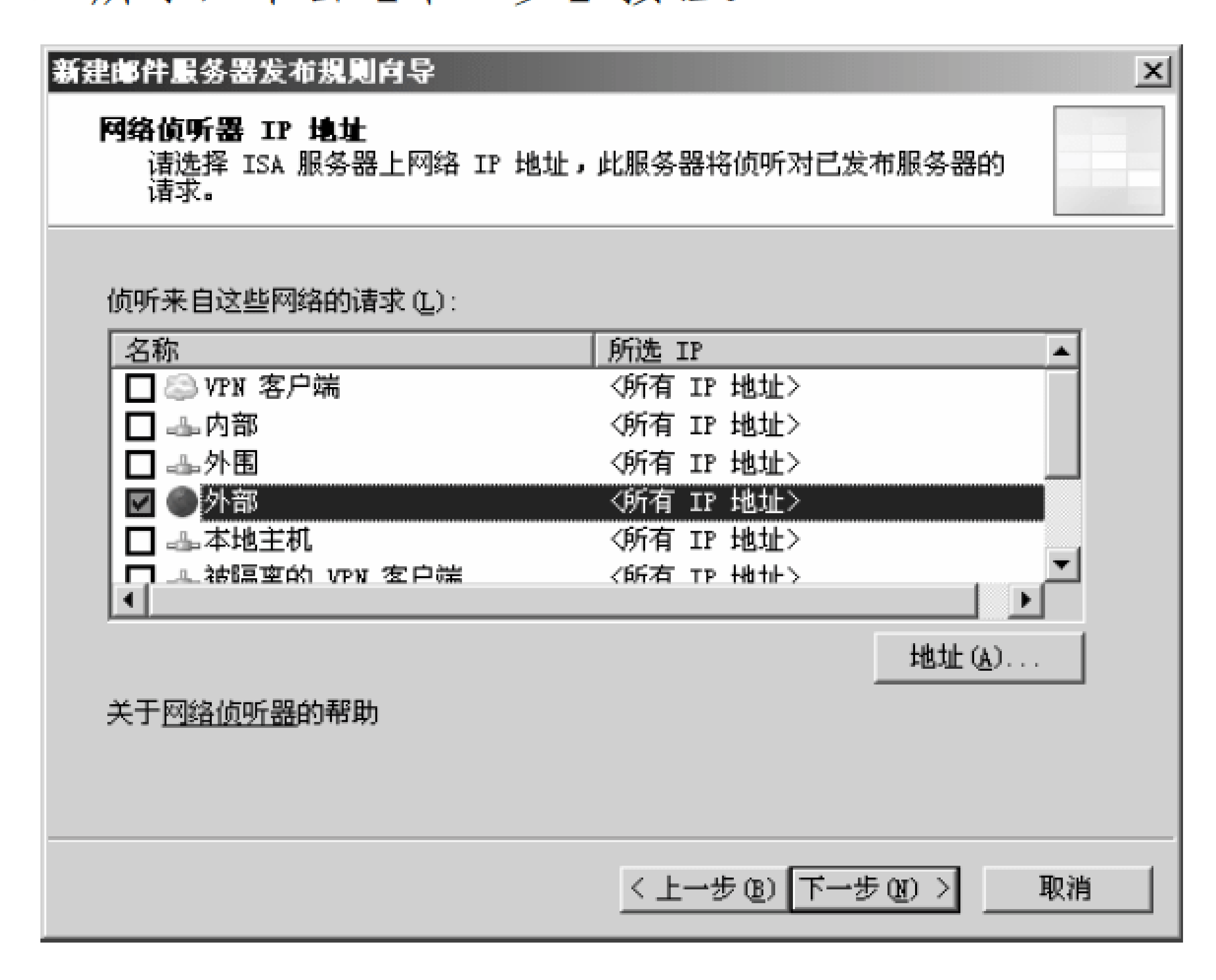


图 14-101

07 配置完成，在弹出的对话框中显示了发布邮件服务器的配置信息，如图 14-102 所示，单击【完成】按钮。

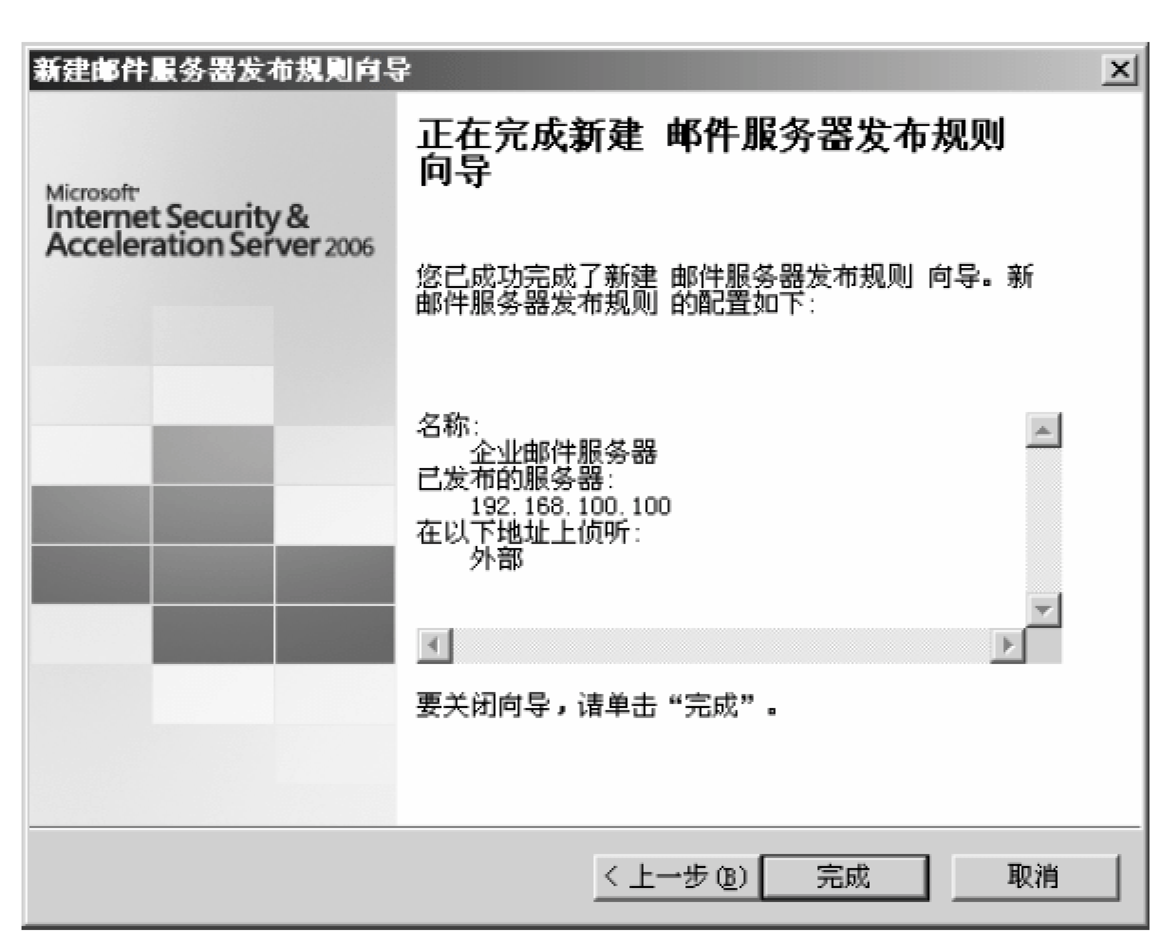


图 14-102

08 返回程序主界面，单击【应用】按钮使配置生效，如图 14-103 所示。



图 14-103

14.4.3 ISA 防火墙安全发布其他服务器

使用 ISA 防火墙发布其他服务器的操作步骤相似，以 DNS 服务器的发布为例，其具体的操作步骤如下。

01 打开程序主界面，在右侧【任务】选项卡中选择【发布非 Web 服务器协议】选项，如图 14-104 所示。

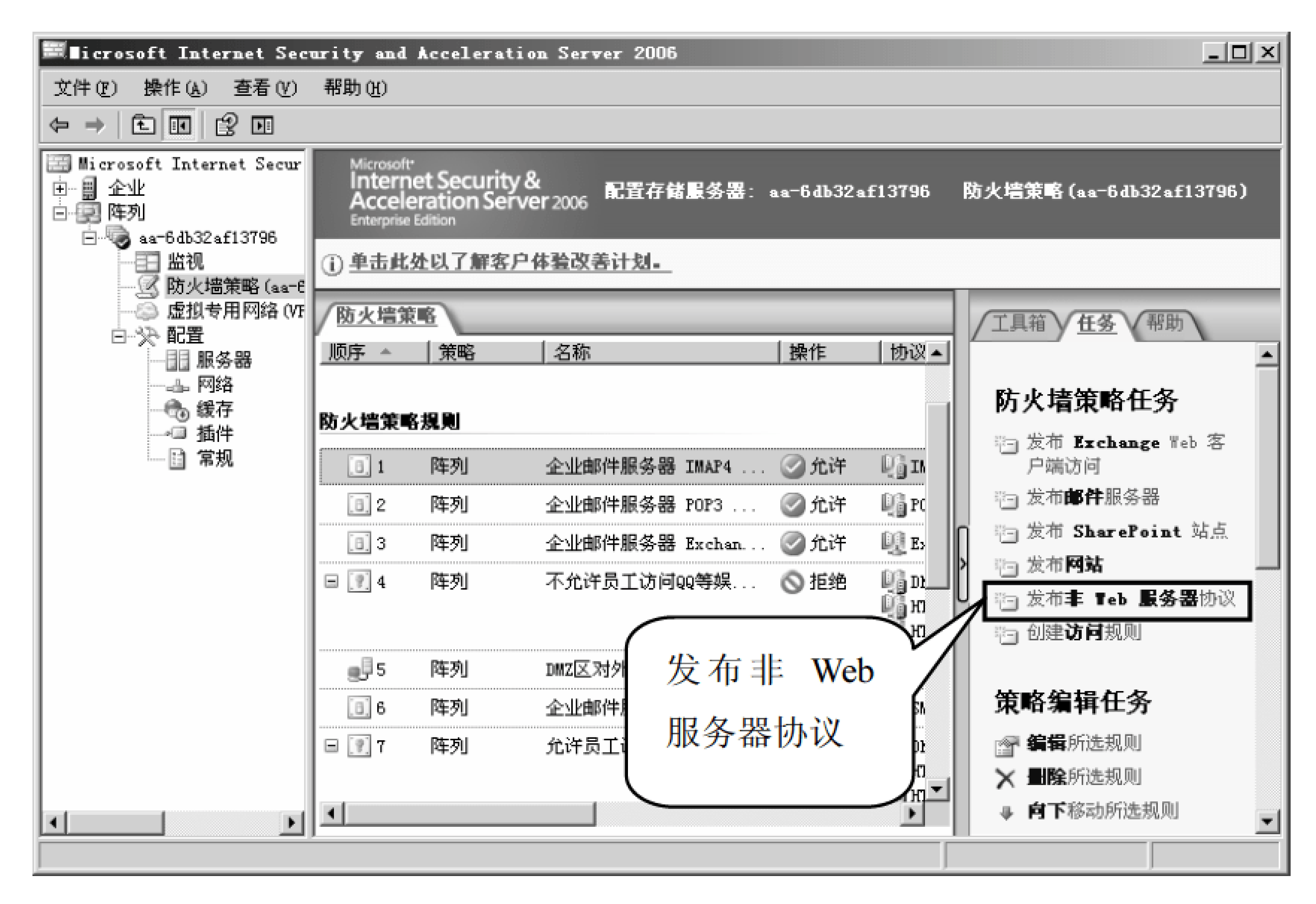


图 14-104

02 弹出【新建服务器发布规则向导】对话框，在【服务器发布规则名称】文本框中输入"企业 DNS 服务器发布"，如图 14-105 所示，单击【下一步】按钮。

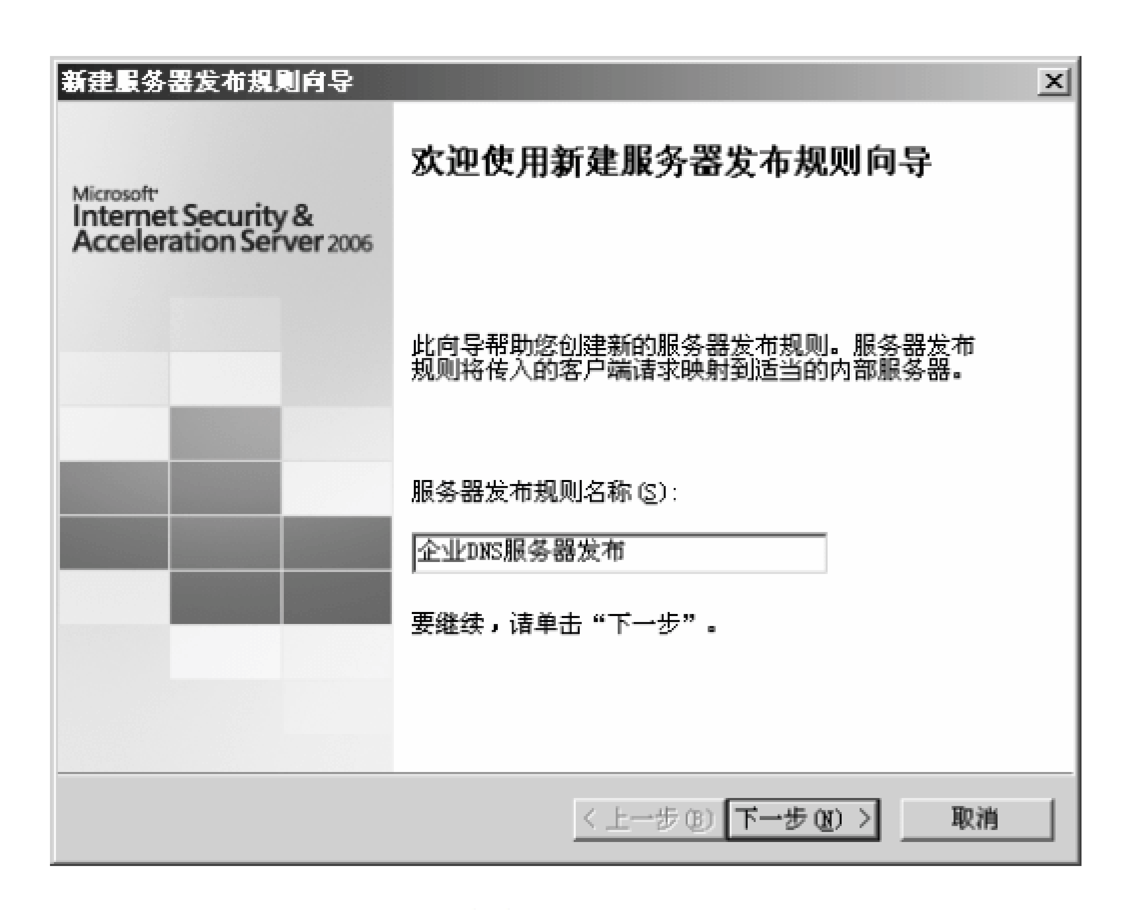


图 14-105

03 弹出【选择服务器】对话框，在【服务器 IP 地址】文本框中输入 DNS 服务器的 IP 地址“192.168.100.100”，如图 14-106 所示，单击【下一步】按钮。



图 14-106

04 弹出【选择协议】对话框，在【选择的协议】下拉选项中选择【DNS 服务器】选项，如图 14-107 所示，单击【下一步】按钮。



图 14-107

05 弹出【网络侦听器 IP 地址】对话框，在【侦听来自这些网络的请求】选项列表中选择【外部】选项，如图 14-108 所示，单击【下一步】按钮。

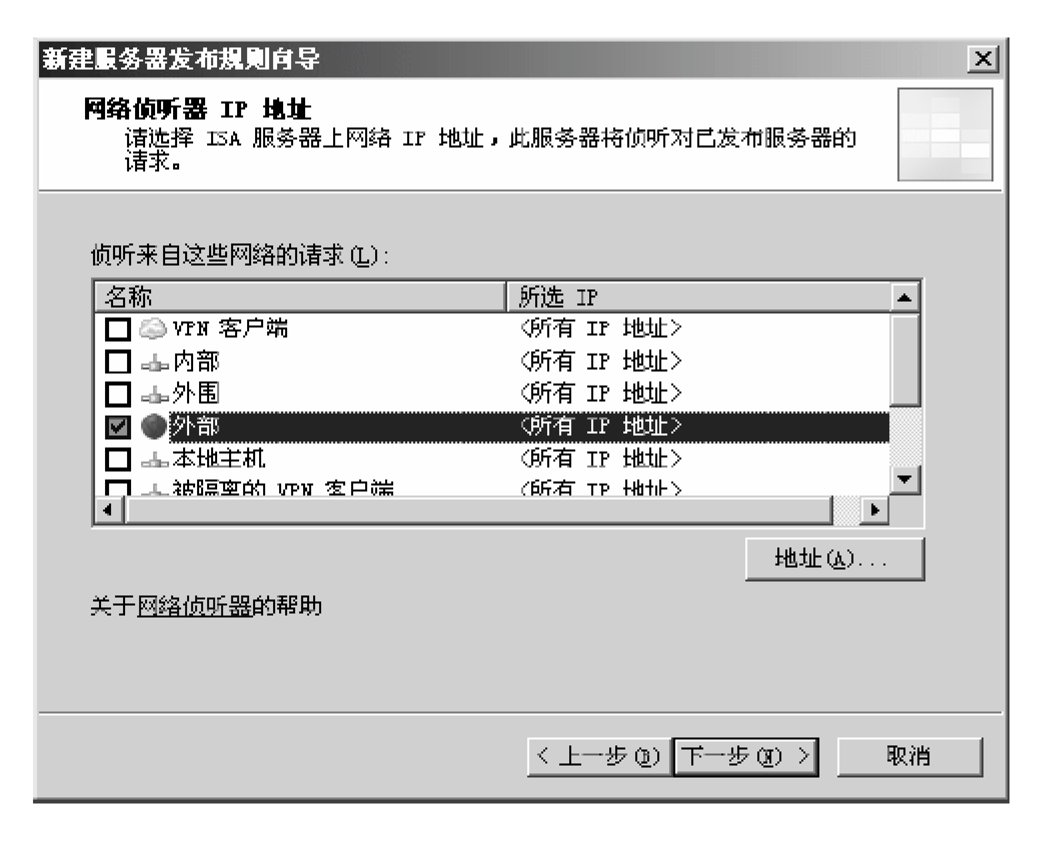


图 14-108

06 配置完成，在弹出的对话框中显示了新发布 DNS 服务器的配置信息，如图 14-109 所示，单击【完成】按钮。

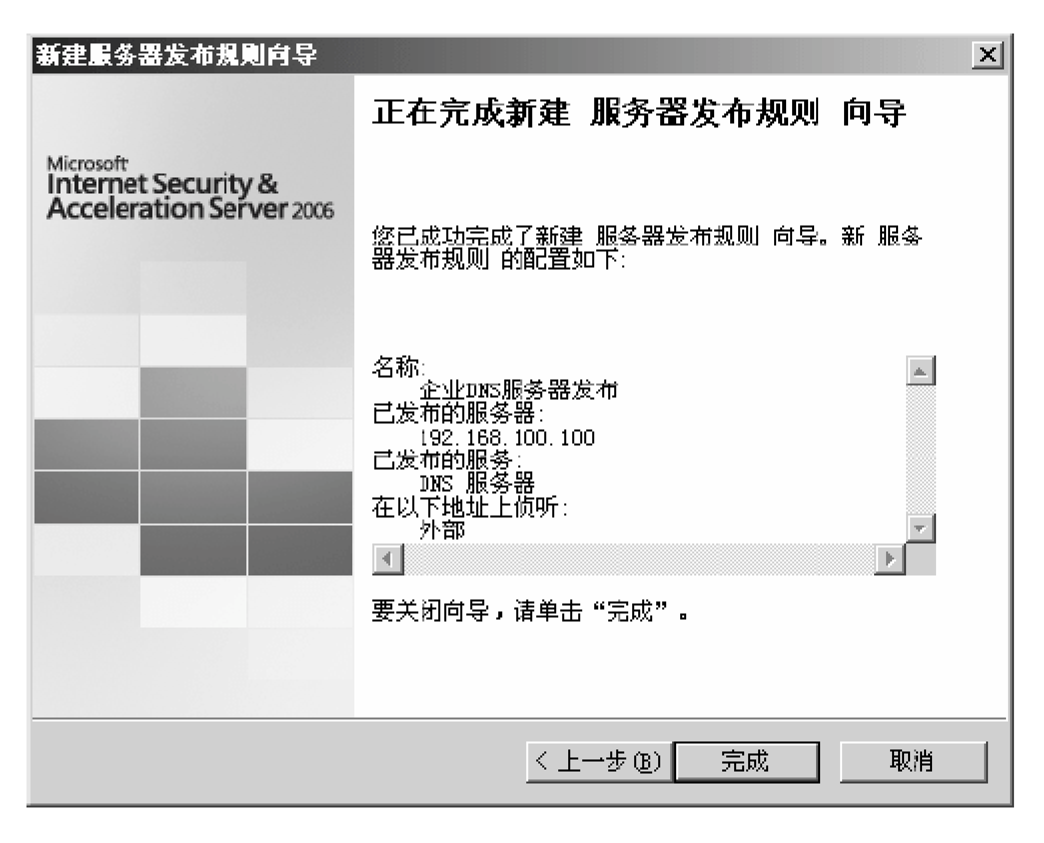


图 14-109

07 返回程序主界面，单击【应用】按钮使配置生效，如图 14-110 所示。

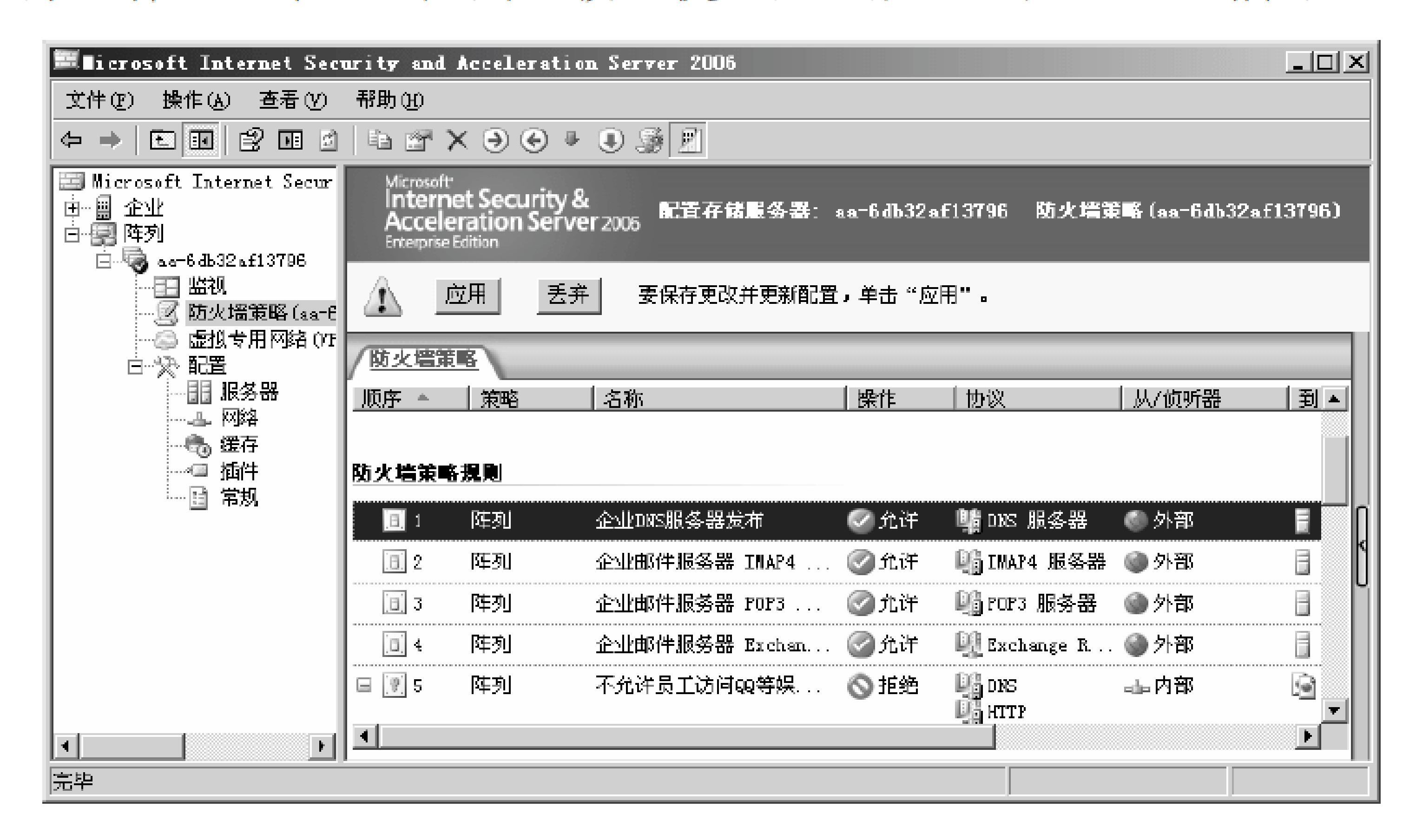


图 14-110

14.5 专家答疑

（1）如果企业使用了出口防火墙部署，个人计算机上还有必要配置防火墙吗？

答：企业防火墙是用来防护外网攻击的，对于内网产生的攻击，防护能力很弱。所以在企业中每一台主机都需要开启个人防火墙，以防护局域网的病毒或木马攻击。同时，个人防火墙还可以防止非法链接。

（2）企业防火墙的访问策略应当按照什么样的原则进行配置？

答：一般默认规则要选择拒绝所有流量，其他流量应该遵循以下两条原则。

①简单实用：防火墙本事已经属于较为复杂的安全设备，其涉及到的技术比较广泛，而很多网络管理人员由于技术水平有限，很难驾驭防火墙。如果配置不慎，出现了配置错误，没有很好的经验，恢复起来会很吃力。所以在配置访问规则的时候，能简化的尽量简化，越简单的实现方式，越容易理解和使用。而且设计越简单，越不容易出错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。虽然简单，但是也要尽量禁止一切无用流量的通信。

防火墙的安全功能很多，但是这些功能并不是所有应用环境都需要，配置时要结合企业需求，不必要的功能尽量使用默认配置，否则会大大增强配置难度，而且还可能因配置不当，引起新的安全漏洞。

②结合全网安全架构需求：很多用户配置防火墙时，只是看到了防火墙本身的防护，配置几条访问策略就了事了。可是网络需要全面的、多层次的防御战略体系才能实现真正的安全。因此，要与入侵检测、网络加密认证、病毒查杀等多种安全措施相结合，才能构建多层次、多角度的安全体系。

第 15 章　企业反病毒

随着互联网的不断发展，病毒也不断演变，新型病毒层出不穷，在网络传播能力和破坏力方面表现的也越来越强劲，因此，反病毒已经成为企业信息安全非常重要的一环。特别是在企业网络里，用户群比较多，安全需求也高，一旦有病毒传播只靠单一主机自主查杀是没有意义的。面对企业网络的病毒威胁，网络管理员必须做更多的考虑，选择更智能、更全面、更系统的企业反病毒系统。

15.1　企业反病毒系统概述

在搭建企业反病毒系统之前，先来了解一下什么是企业反病毒系统，以及其分类、设计原则等信息。

15.1.1　什么是企业反病毒系统

企业反病毒系统是针对企业网络反病毒需要提出的一套可以实时监控网络安全状态，并能实现全网病毒查杀的反病毒系统。

要想深刻地了解什么是企业反病毒系统，首先要把企业反病毒系统和通常个人家庭使用的杀毒软件区分开。比如常见的个人家庭使用的瑞星、360、卡巴斯基、金山等杀毒软件，都是针对单个主机进行查杀病毒的。常见的企业反病毒系统有诺顿企业版、ESET NOD32 企业版、卡巴斯基企业版、360 杀毒企业版、趋势科技等。

15.1.2　企业反病毒系统的设计原则

面对如此严峻的网络安全形势，各大企业对网络信息安全防护也越来越重视，并纷纷投入大笔资金进行网络安全产品的采购和部署。但是设备只是信息安全防护的骨架，应该有合理的、统一的防范策略作保障。所以在架设反病毒系统时需要进行严格的、深入的分析和设计。

下面详细介绍企业防病毒系统的设计原则。

1. 满足查杀中国式病毒要求

文化有国界特色，病毒也不例外，中国式病毒在网络安全部署过程中是不容忽视的。所以在进行反病毒系统设计时也需要考虑中国特色。

国际上知名的老牌杀毒软件，拥有强大的软硬件技术，但是面对中国式病毒也无能为力。

2006~2007 年比较流行的熊猫烧香病毒，大都是依靠 360 等多款国内杀毒软件推出的专杀程序解决的。不是说国外杀毒软件不好，只是在针对中国特色病毒上，它们没有突出优势。

所以在国内网络中可以使用国际知名的老牌杀毒软件，但是也要在此基础上做好中国式病毒查杀的补充。

2. 保证对新病毒的查杀能力

杀毒软件并不是安装之后就不用理会了，随着新病毒、木马的不断出现，杀毒软件也必须及时的更新程序和病毒库。如果不能实现快速的升级和病毒库更新，新病毒就会以其惊人的传播速度和破坏力毁灭整个网络的计算机，给企业带来巨大的损失。所以保证杀毒软件快速的升级和响应是体现其病毒查杀能力的决定性因素之一。

杀毒软件的升级和病毒库更新由三方面因素决定：软件因素、管理因素和网络因素。

（1）软件因素：不同的软件应对新病毒的更新速度不相同，选择一款更新及时的杀毒软件很重要，很多软件可以做到一天几次的更新频率。

（2）管理因素：很多杀毒软件被设置为更新需要管理员手动操作，比如需要管理员确认更新提示等，这样会影响更新速度，一般建议设定为自动更新，且每天做一次手动更新。

（3）网络因素：网络环境通畅与否也直接影响着更新效率，如网络经常处于拥塞、速率低等状态，则更新效率会降低。

15.2 项目实施 1：ESET NOD32 企业反病毒系统实战案例

ESET NOD32 作为知名的企业反病毒系统，具有较高的市场占有率。下面介绍 ESET NOD32 企业反病毒系统的架设及应用。

15.2.1 安装 ESET NOD32 企业反病毒系统

ESET NOD32 企业反病毒系统主要由三部分程序组成：ESET NOD32 防病毒软件、ESET 远程管理服务器、ESET 远程管理控制台。这三个软件可以通过官方网站下载获得。

企业内所有客户机都需要安装 ESET NOD32 防病毒软件，同时需要指定一台主机安装 ESET 远程管理服务器和 ESET 远程管理控制台程序，作为企业反病毒系统的管理服务器。

下面分别介绍三种程序的安装过程等。

1. 安装 ESET NOD32 企业版防病毒软件

安装 ESET NOD32 防病毒软件之前，一定要确保本机没有其他安全防护程序，如病毒防护和间谍软件防护程序等。安装 ESET NOD32 防病毒软件的具体操作如下。

01 运行 ESET NOD32 防病毒软件安装程序，弹出安装向导对话框，如图 15-1 所示，单击【下一步】按钮。



图 15-1

02 弹出【最终用户许可协议】对话框，选择【我接受许可协议中的条款】单选按钮，如图 15-2 所示，单击【下一步】按钮。

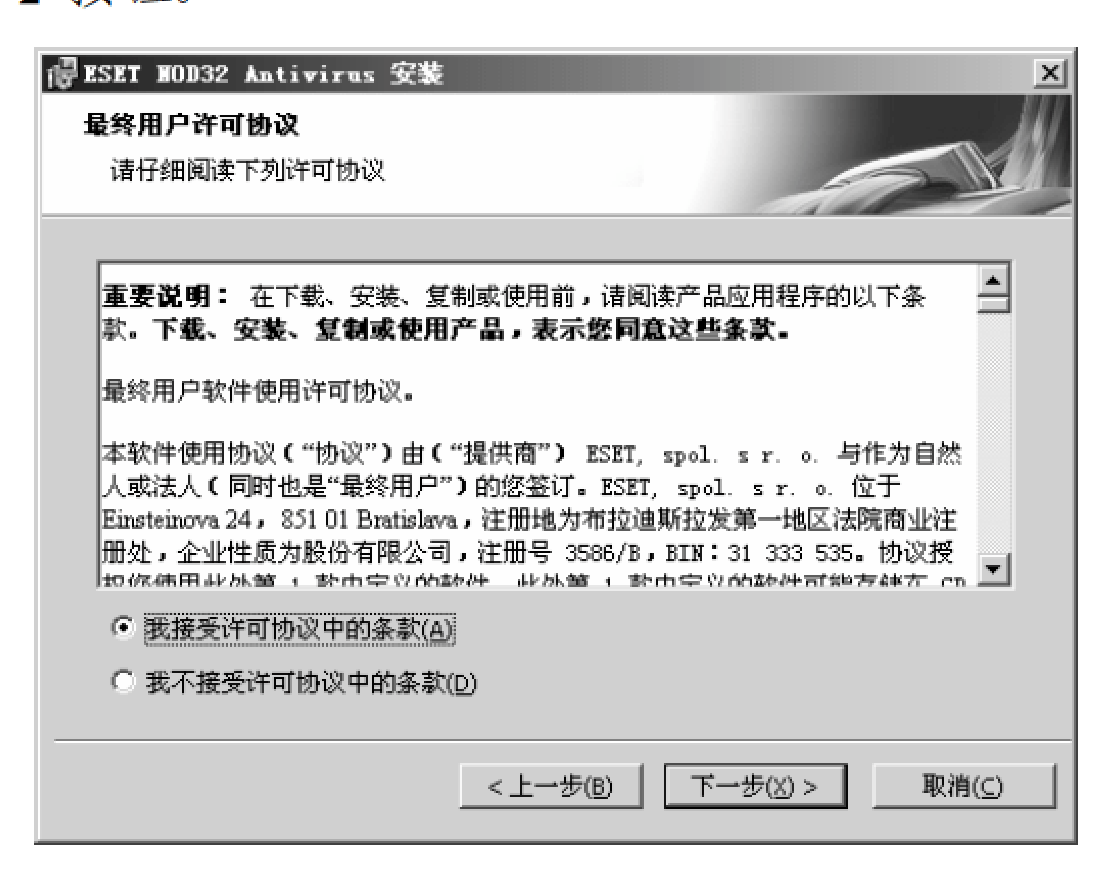


图 15-2

03 弹出【安装模式】对话框，根据个人情况选择安装模式，如果是初学者建议选择【典型】模式，如图 15-3 所示，单击【下一步】按钮。



图 15-3

04 弹出【自动更新】对话框，病毒软件需要及时更新程序及病毒库，在更新时需要向服务器提供有效的用户名及密码，在【用户名】和【密码】文本框分别输入已获得的用户名及密码信息，如果还没有用户名和密码可选择【以后再设置用户名和密码】复选框，如图 15-4 所示，单击【下一步】按钮。

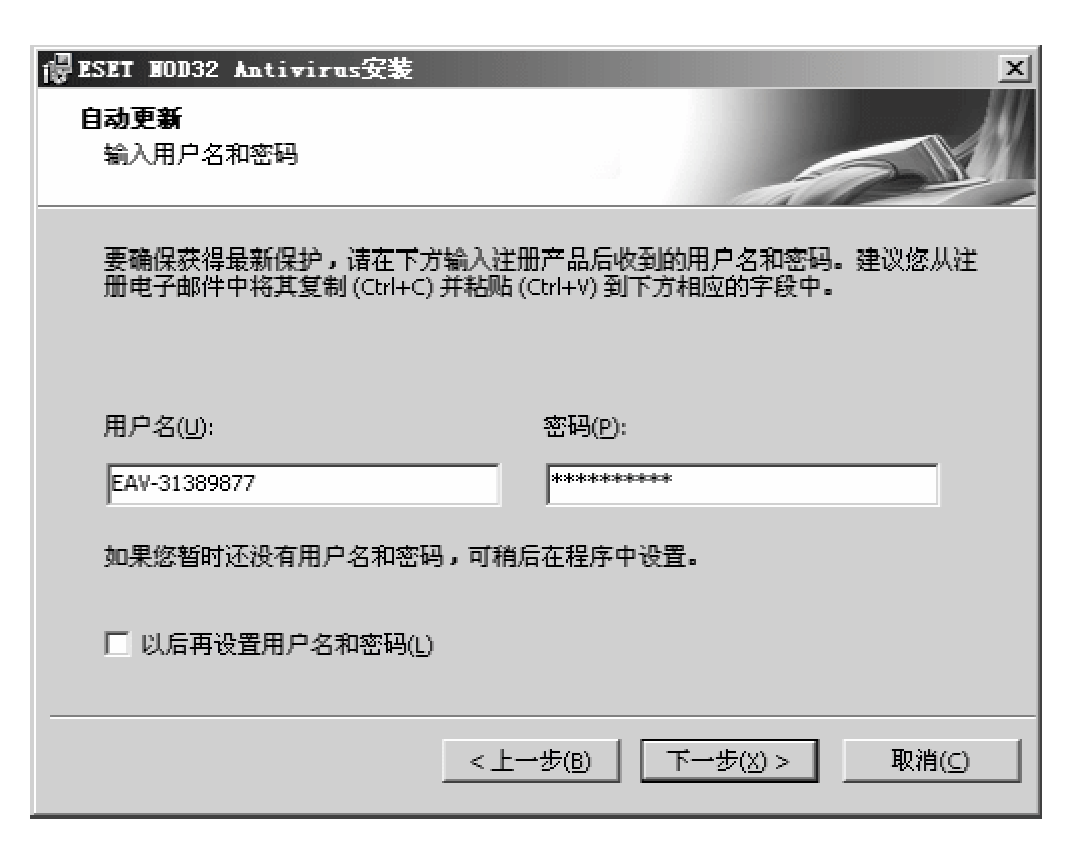


图 15-4

05 弹出【ThreatSense.Net 预警系统】对话框，通过该项配置可以及时提交系统遇到的最新威胁给 ESET 实验室，选择【启用 ThreatSense.Net 预警系统】复选框，并采用默认配置，如图 15-5 所示，单击【下一步】按钮。

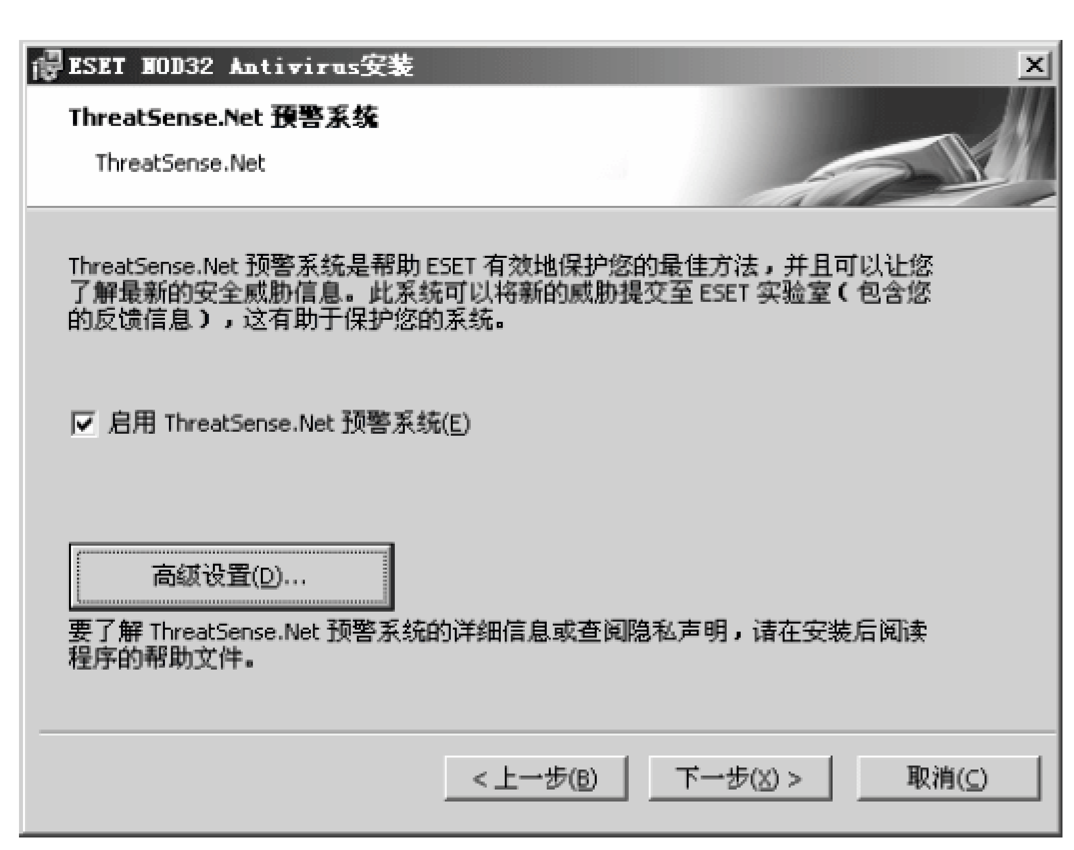


图 15-5

06 弹出【检测潜在不受欢迎的应用程序】对话框，为了使计算机的性能、速度及可靠性更高，建议选择【启用潜在不受欢迎的应用程序检测功能】下拉菜单选项，如图 15-6 所示，单击【下一步】按钮。



图 15-6

07 安装基本配置已经完成，弹出【准备安装】对话框，如图 15-7 所示，单击【安装】按钮。



图 15-7

08 系统自动安装程序，并显示安装进度，如图 15-8 所示，也可以单击【取消】按钮撤销本次安装。



图 15-8

09 安装结束，如图 15-9 所示，单击【完成】按钮，完成安装向导。



图 15-9

2. 安装远程管理服务器

ESET 远程管理服务器必须在指定的管理主机上安装，具体的安装步骤如下。

01 运行 ESET 远程管理服务器安装程序，弹出安装向导对话框，如图 15-10 所示，单击【下一步】按钮。



图 15-10

02 弹出【最终用户许可协议】对话框，选择【我接受许可协议中的条款】单选按钮，如图 15-11 所示，单击【下一步】按钮。

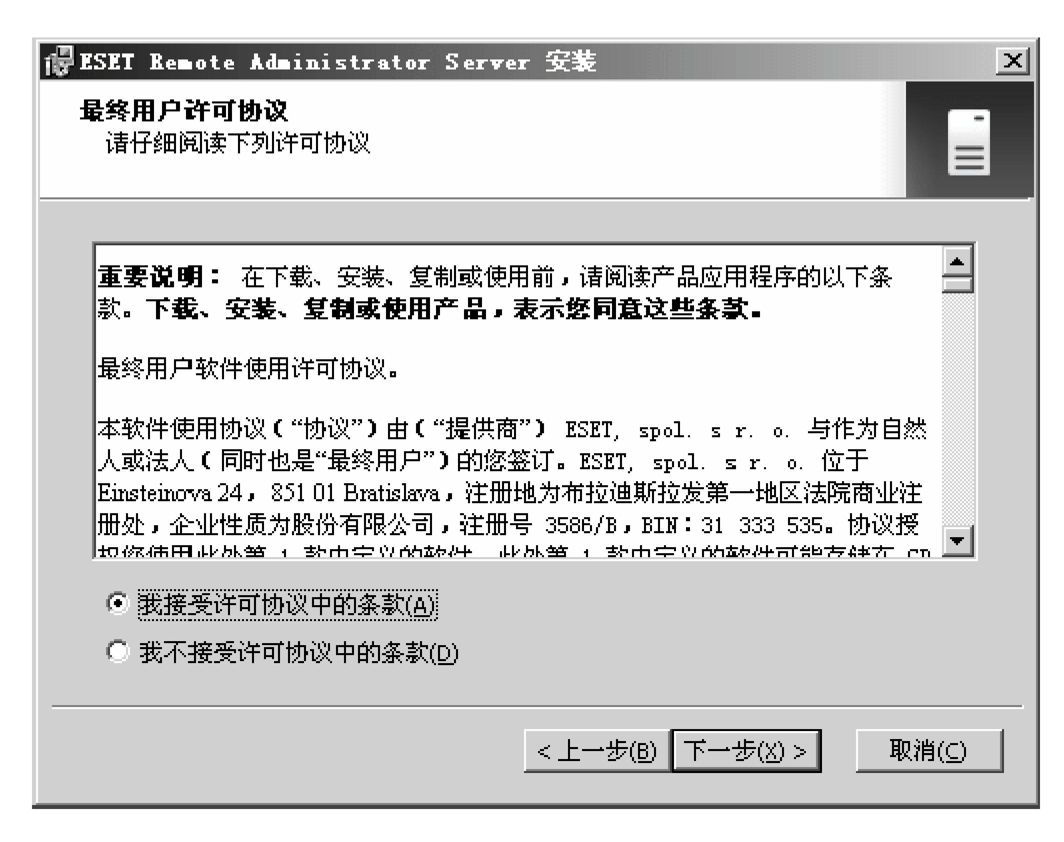


图 15-11

03 弹出【选择安装类型】对话框，根据个人情况选择安装类型，如果是初学者建议选择【典型】模式，如图 15-12 所示，单击【下一步】按钮。



图 15-12

04 弹出【许可证密钥】对话框，单击【浏览】按钮选择已经获得的“lic”后缀的许可证密钥文件，添加成功后显示出该密钥支持的【产品】、【客户】及【到期日期】等信息，如图 15-13 所示，单击【下一步】按钮。

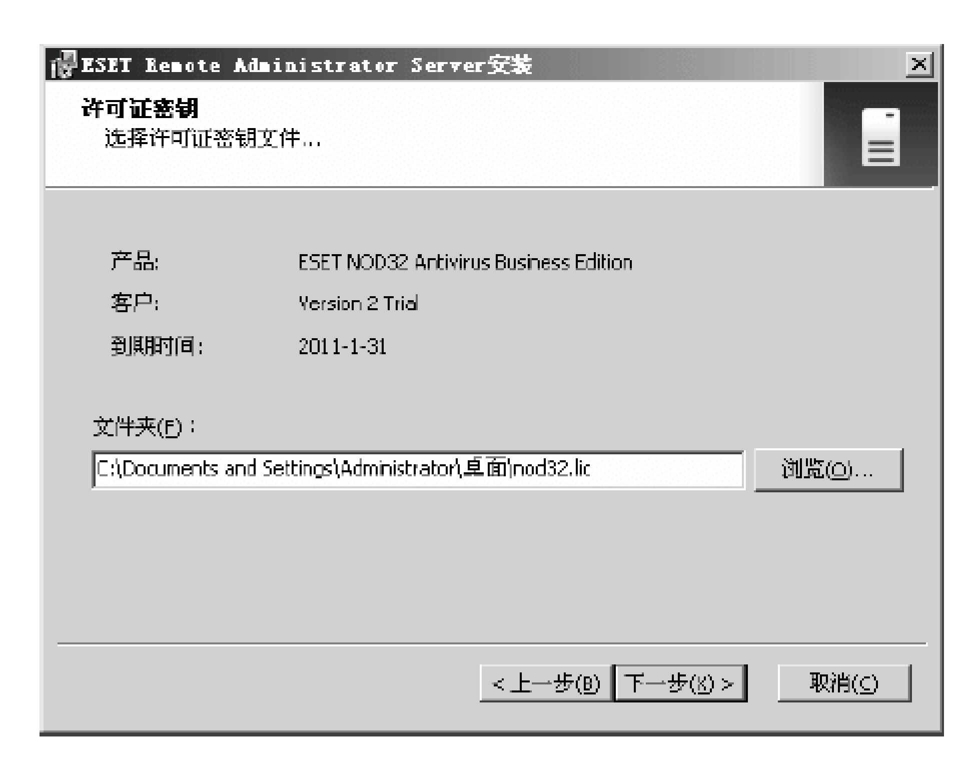


图 15-13

05 弹出【安全设置】对话框，单击【设置】按钮，可分别设置控制台管理员权限密码、控制台只读权限密码、远程代理安装程序密码、客户端密码、客户端和服务器同步密码，如图 15-14 所示，建议使用文档将密码妥善保管，配置完成后单击【下一步】按钮。

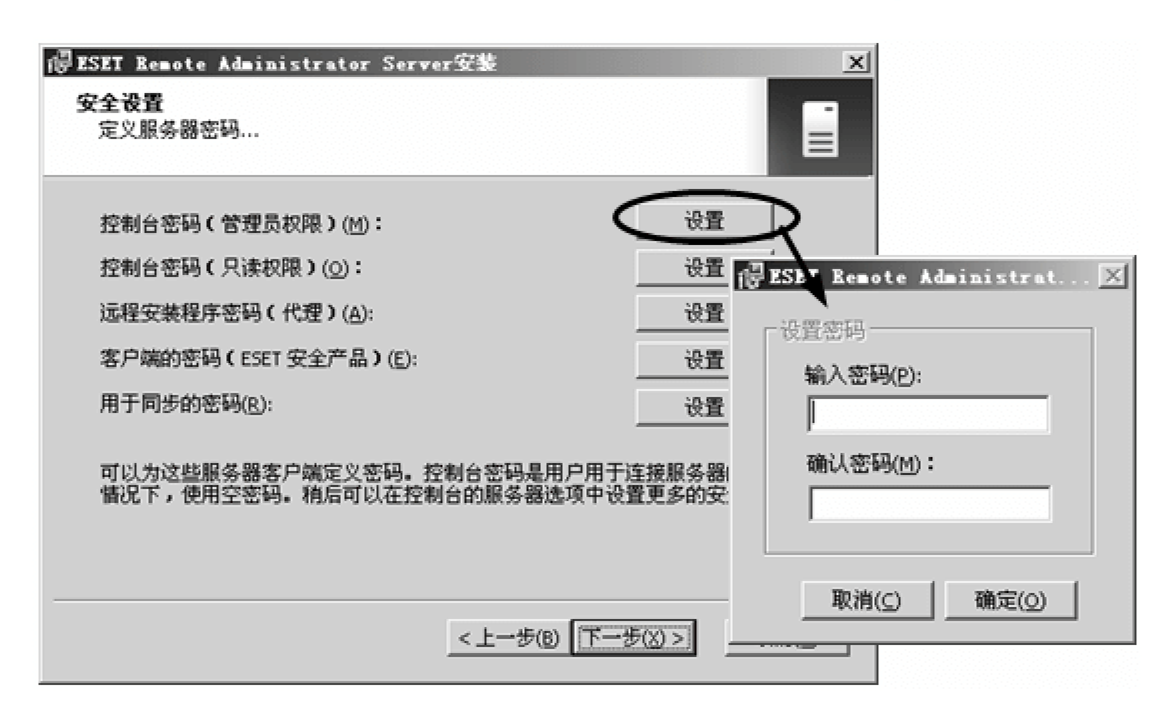


图 15-14

06 弹出【更新】对话框，选择【以后再设置更新参数】复选框，如图 15-15 所示，单击【下一步】按钮。

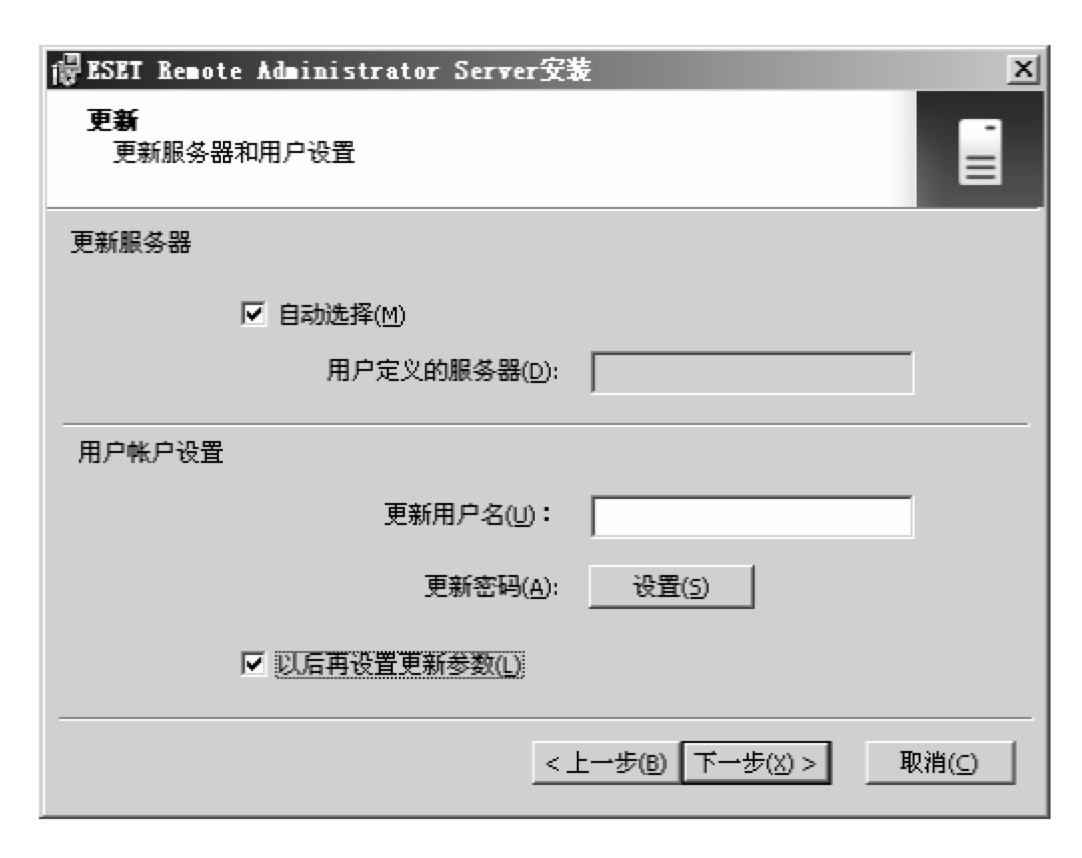


图 15-15

07 安装基本配置已经完成，弹出【准备安装】对话框，如图 15-16 所示，单击【安装】按钮。



图 15-16

08 系统自动安装程序，并显示安装进度，如图 15-17 所示，也可以单击【取消】按钮撤销本次安装。

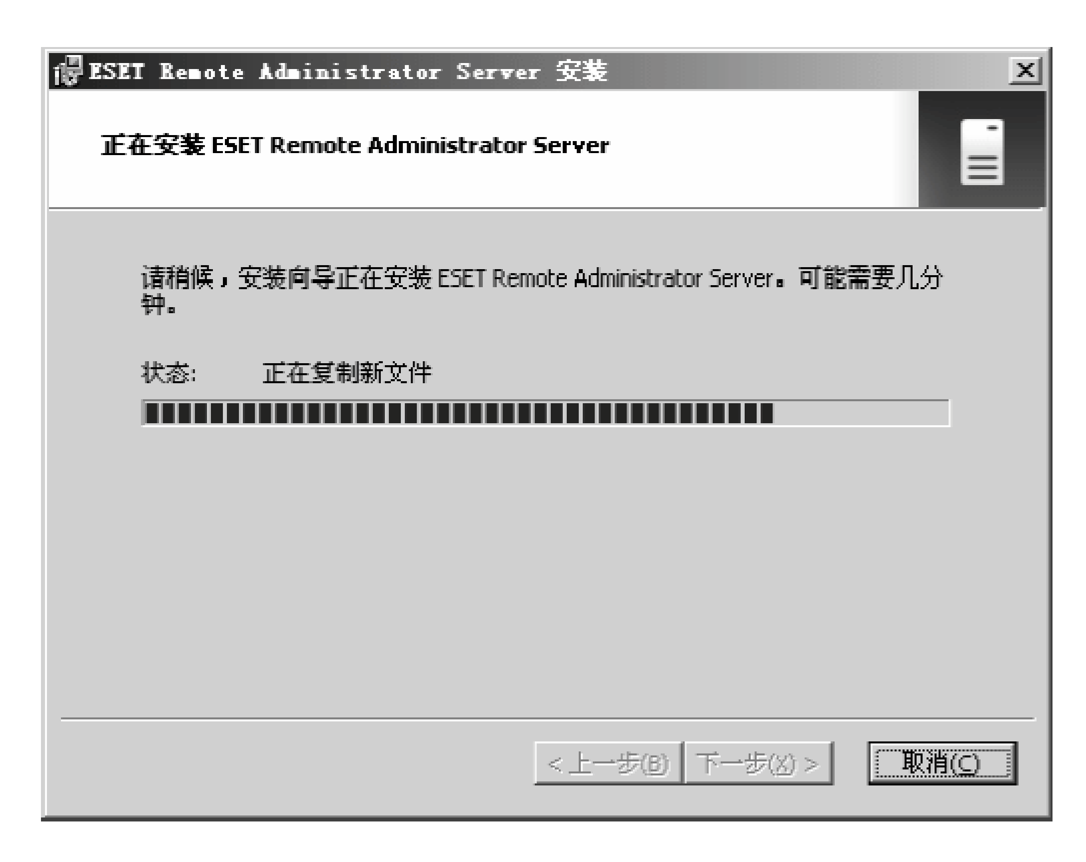


图 15-17

09 安装结束，单击【完成】按钮，完成安装向导，如图 15-18 所示。



图 15-18

3. 安装管理控制台

安装 ESET 管理控制台的主机要和安装 ESET 管理服务器的主机是同一台，其具体的安装步骤如下。

01 运行 ESET 管理控制台安装程序，弹出安装向导对话框，如图 15-19 所示，单击【下一步】按钮。



图 15-19

02 弹出【最终用户许可协议】对话框，选择【我接受许可协议中的条款】单选按钮，如图 15-20 所示，单击【下一步】按钮。

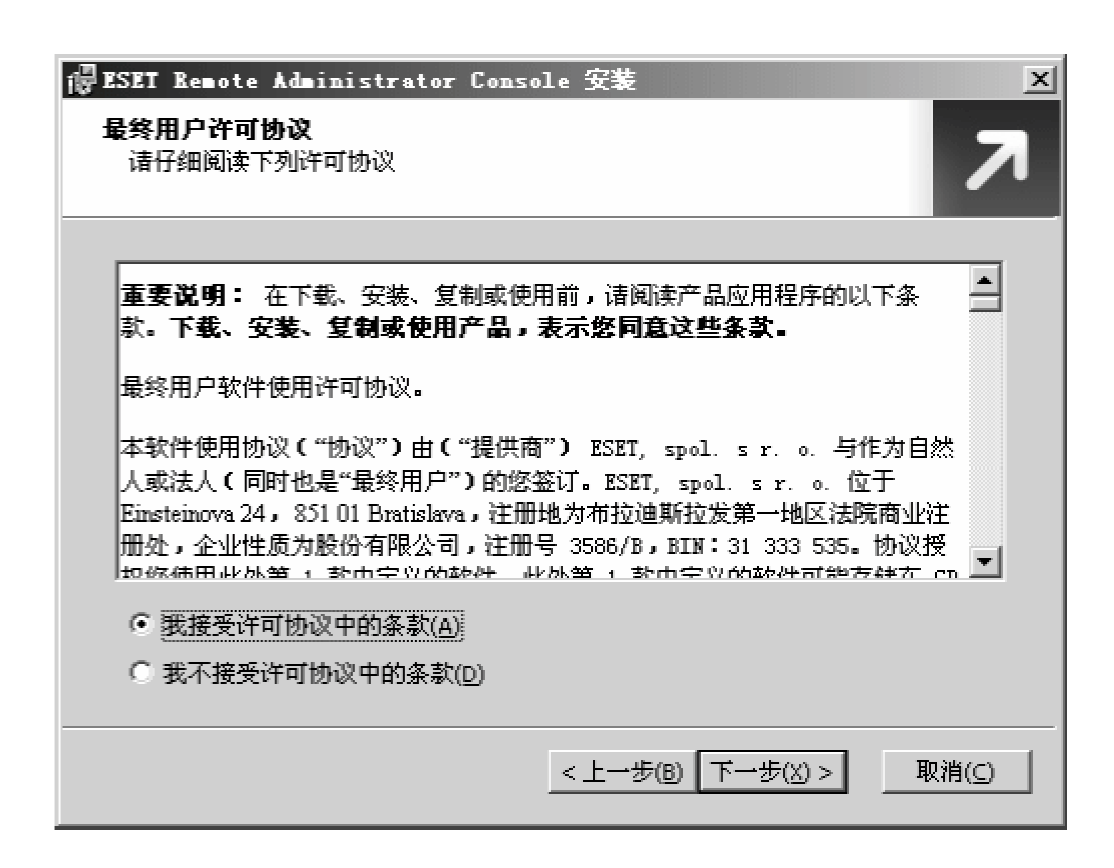


图 15-20

03 弹出【选择安装类型】对话框，根据个人情况选择安装类型，如果是初学者建议选择【典型】模式，如图 15-21 所示，单击【下一步】按钮。



图 15-21

04 弹出【选择安装文件夹】对话框，在【文件夹】文本框中输入程序安装目录，也可以单击【浏览】按钮指定安装目录，本实例采用默认配置，如图 15-22 所示，单击【下一步】按钮。



图 15-22

05 安装基本配置已经完成，弹出【准备安装】对话框，单击【安装】按钮，如图 15-23 所示。



图 15-23

06 系统自动安装程序，并显示安装进度，如图 15-24 所示，可以单击【取消】按钮撤销本次安装。



图 15-24

07 安装结束，单击【完成】按钮，完成安装向导，如图 15-25 所示。



图 15-25

15.2.2 设置 ESET 配置编辑器

在企业版中，需要通过管理控制台对所有反病毒客户机进行管理，管理控制台在使用之前需要先做基础管理配置，主要是对配置编辑器进行配置。通过配置编辑器可以更改客户端的配置，给客户端新增计划任务等。配置编辑器的配置内容比较多，本实例主要介绍两部分：分别是 ESET 内核和升级设置。

1. 打开配置编辑器

在设置 ESET 内核和升级之前，需要打开配置编辑器，具体的操作步骤如下。

01 双击桌面上的远程管理控制台程序【ESET Remote Administrator Console】的快捷方式，打开控制台程序主界面，弹出【输入服务器密码】对话框，【服务器】、【类型】和【访问权限】三项默认产生，只需要在【密码】文本框中输入安装程序时设置的密码即可，输入密码后单击【确定】按钮，如图 15-26 所示。

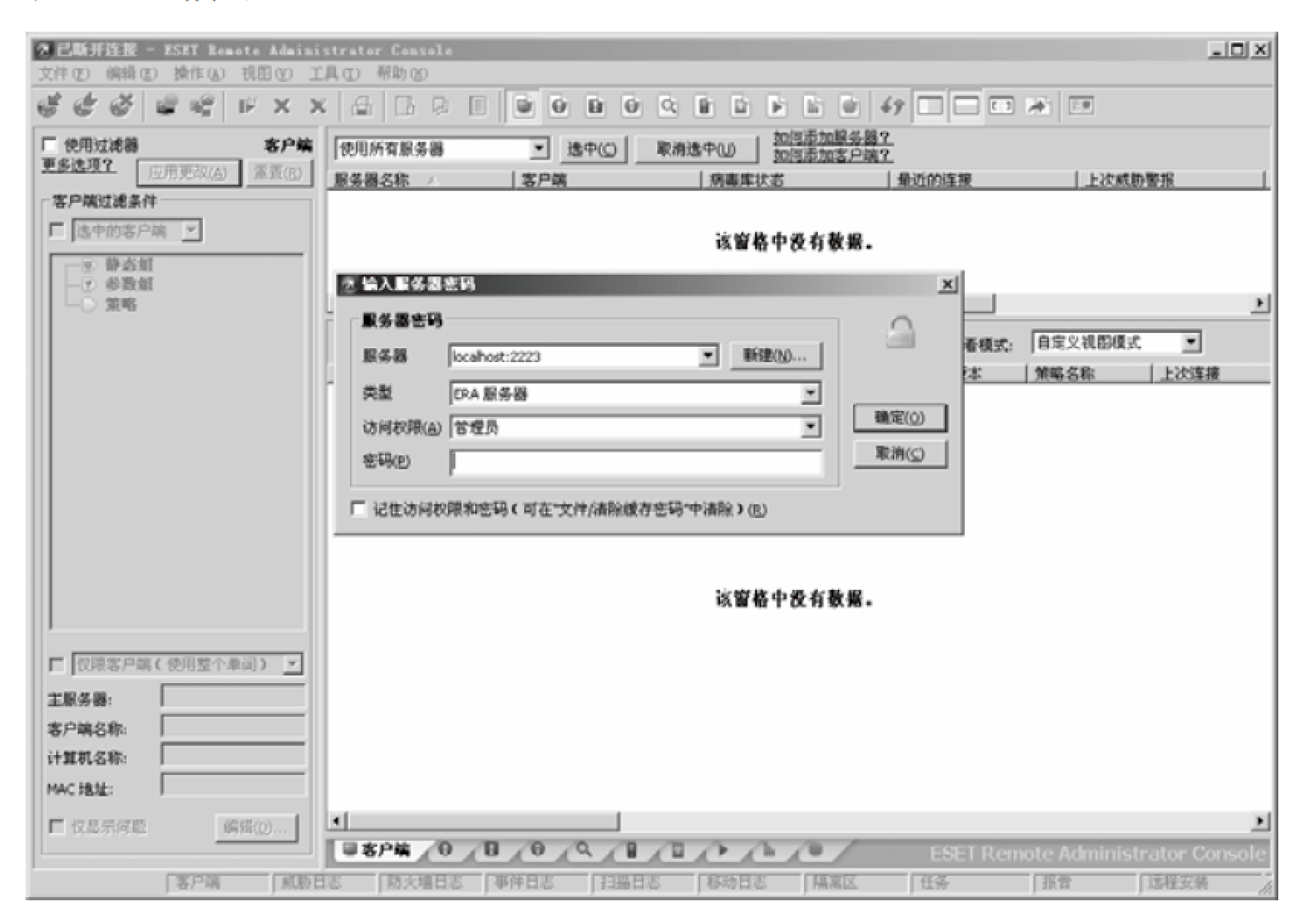


图 15-26

02 密码验证成功后，选择【工具】➢【ESET 配置编辑器】菜单命令，如图 15-27 所示。

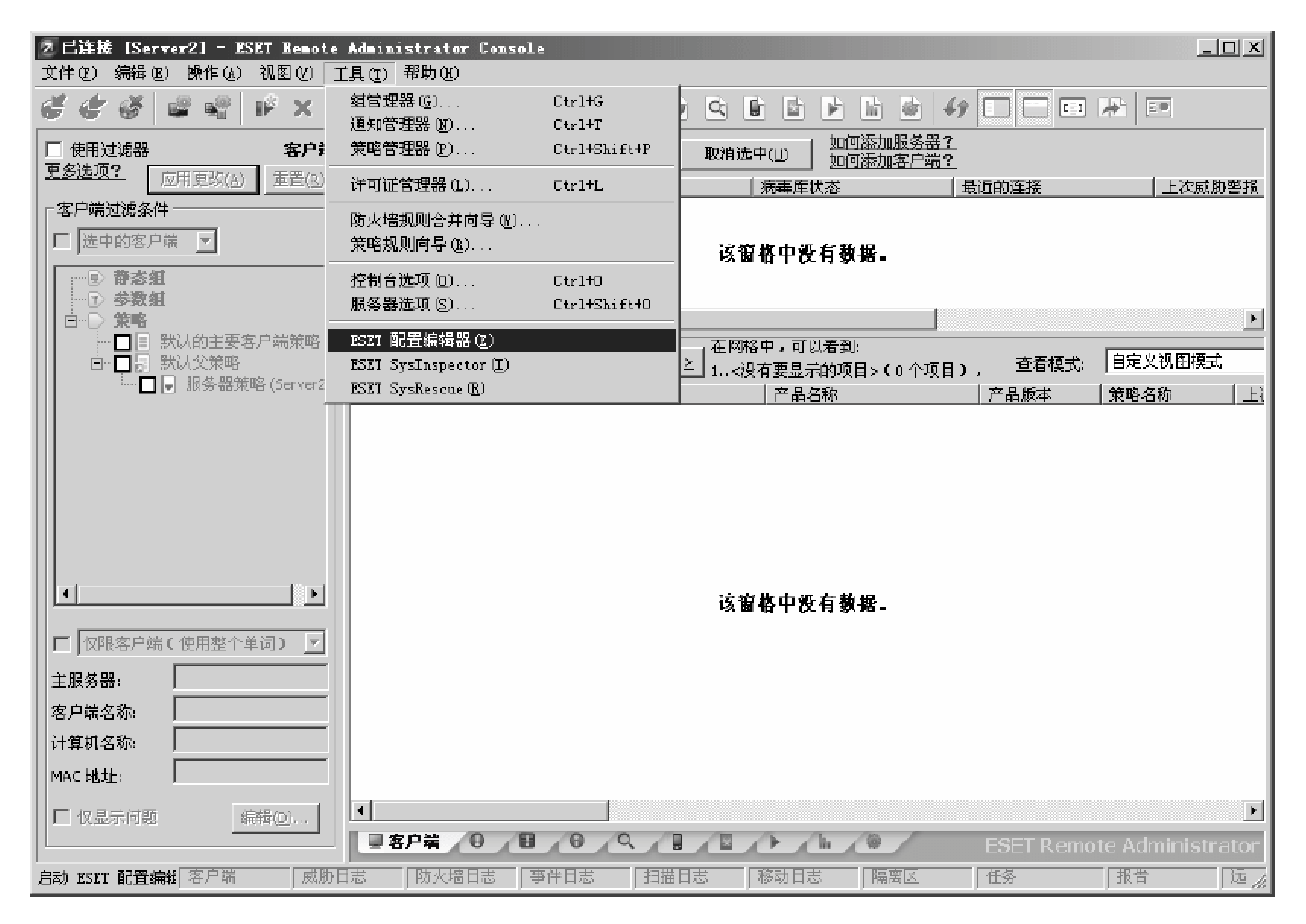


图 15-27

03 弹出【ESET 配置编辑器】窗口。配置编辑器左侧以树状结构显示配置内容，大部分的配置都在【ESET Smart Security,ESET NOD32 Antivirus】这一部分里，所以本实例只对这部分进行配置，如图 15-28 所示。



图 15-28

2. 设置 ESET 内核

在 ESET 内核配置中，主要配置以下三项内容。

（1）远程管理用于指定工作站要连接的远程管理服务器的地址。

具体的配置步骤如下。

01 选择【ESET 内核】➢【设置】➢【远程管理】选项，显示出【远程管理】配置项的配置内容，如图 15-29 所示。



图 15-29

02 选择【连接到 Remote Administrator Server】选项，勾选右侧【值】复选框，如图 15-30 所示，使管理控制台连接到管理服务器。



图 15-30

03 选择【主服务器地址】选项，在右侧【值】文本框中输入客户机需要连接的服务器 IP 地址，本实例采用“192.168.1.102”，如图 15-31 所示。



【远程管理】中的其他选项可以根据实际情况配置，其中【主服务器端口】的值是客户端连接到远程管理服务器的默认端口，如果在远程管理服务器上安装了防火墙，需要设定防火墙允许该端口流量通信，否则客户端是连接不上的。



图 15-31

（2）设置保护参数

可以设置保护密码，客户端获得保护密码后可以起到保护作用。可以防止客户端配置被随意更改，防止客户端被卸载等。

设置保护参数的具体操作步骤如下。

01 选择【ESET 内核】➢【设置】➢【保护设置参数】➢【要解除锁定的密码】选项，单击右侧【设置密码】按钮，如图 15-32 所示。

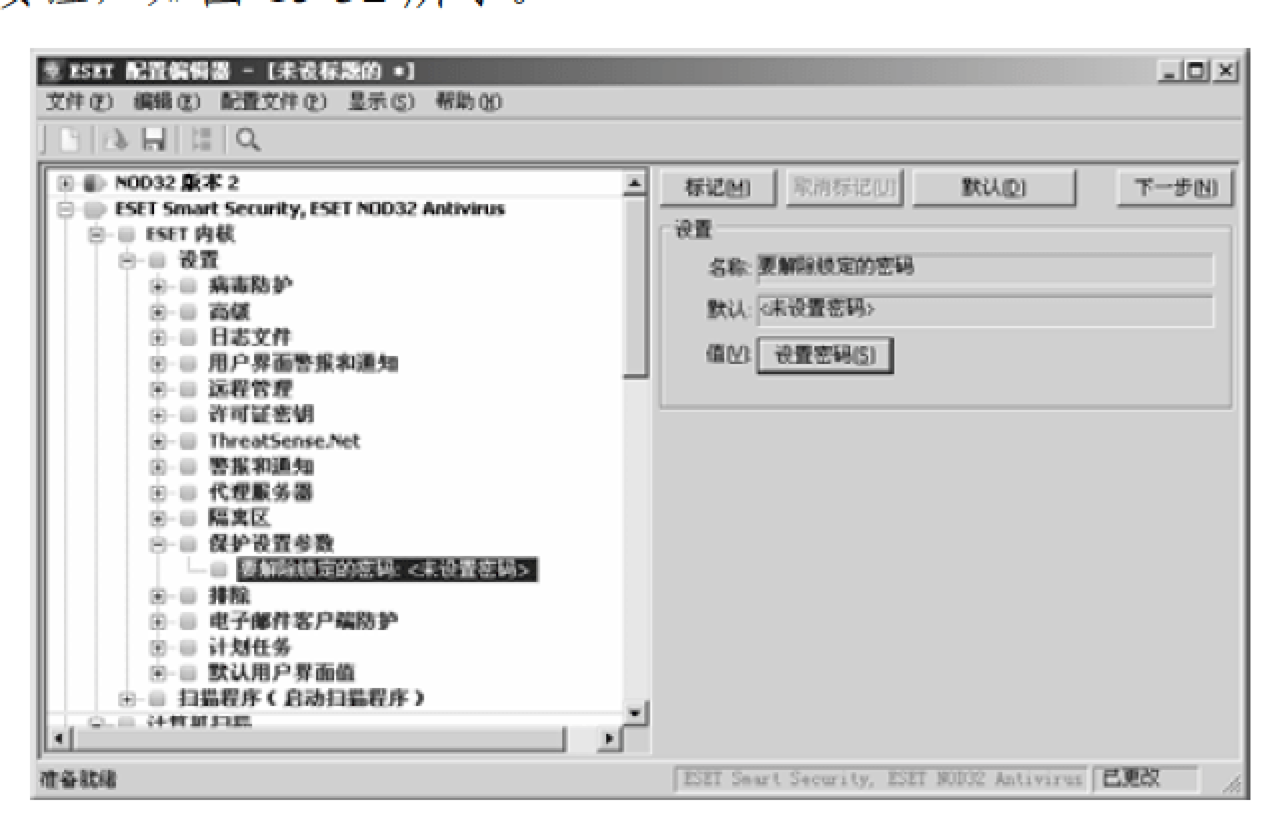


图 15-32

02 弹出【密码】对话框，如图 15-33 所示，在【输入密码】和【确认密码】文本框输入具有较高安全性的密码，不可使用如“123456”一样的简单密码，单击【确定】按钮。



图 15-33

03 设置密码成功，在【要解除锁定的密码】后出现密码字符串“******”，如图 15-34 所示。



图 15-34

（3）计划任务

管理员不可能时刻在管理控制台面前管理客户机，对于一些常规管理任务，应尽量由服务器自己完成，同时企业员工的计算机水平差异很大，管理员应定期对所有客户机进行病毒查杀。考虑这些需求，制作计划任务显得很重要，制作好的计划任务会自动分发到所有客户机。

制作计划任务的具体操作步骤如下。

01 选择【ESET 内核】➢【设置】➢【计划任务】➢【计划任务：总计 0/0（任务/要删除）】选项，单击右侧【编辑】按钮，如图 15-35 所示。



图 15-35

02 弹出【计划任务】对话框，单击【添加】按钮，如图 15-36 所示。



图 15-36

03 弹出【添加任务】对话框，在【计划的任务】下拉菜单选项中可以选择要执行的任务类型，如图 15-37 所示。

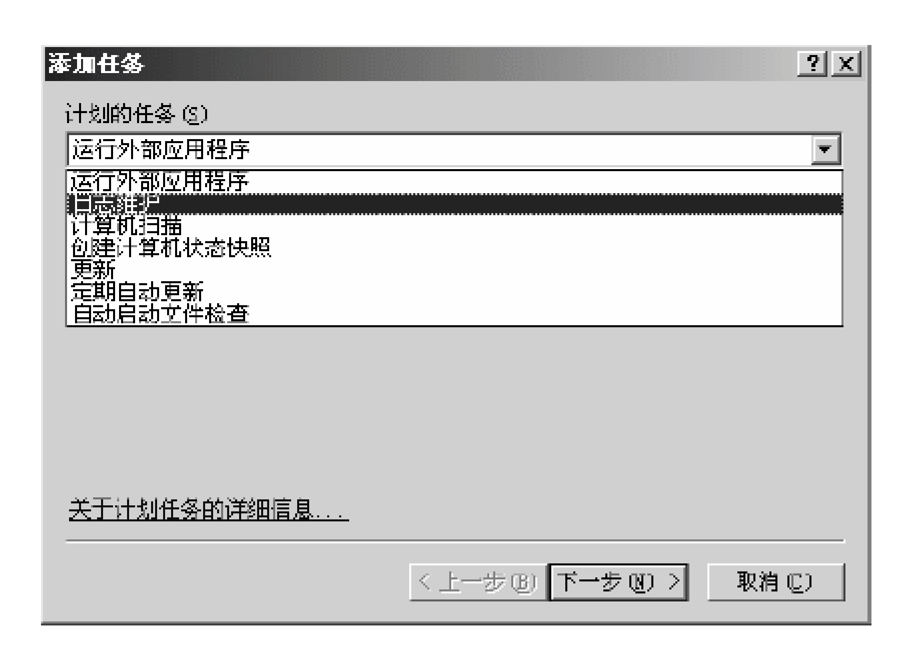


图 15-37

下拉菜单中各项的参数含义如下。

- 【运行外部应用程序】：可以让客户端按照计划运行其他外部程序，这个功能使用比较少。
- 【日志维护】：定期进行日志维护，特别是大型企业，新日志产生的速度很快，如果长期不做清理，会占用很多空间。
- 【计算机扫描】：定时扫描计算机，并按照要求查杀病毒。
- 【创建计算机状态快照】：可按照计划对计算机状态进行周期性快照记录。
- 【更新】：即定时更新病毒库，默认情况下 ESET NOD32 会每个小时自动更新病毒库，所以此功能可以不用设置。
- 【自动启动文件检查】：计算机启动时，自动扫描启动文件，防止病毒在计算机启动时运行，并查杀启动文件夹中的病毒。

04 在【计划的任务】下拉列表选项中选择【计算机扫描】选项，如图 15-38 所示，每周进行一次计算机扫描，单击【下一步】按钮。



图 15-38

05 在弹出的对话框的【任务名称】文本框中输入本次计划任务的名称，本实例输入“每周扫描”，并在【执行任务】中单击【每周】单选按钮，单击【下一步】按钮，如图 15-39 所示。

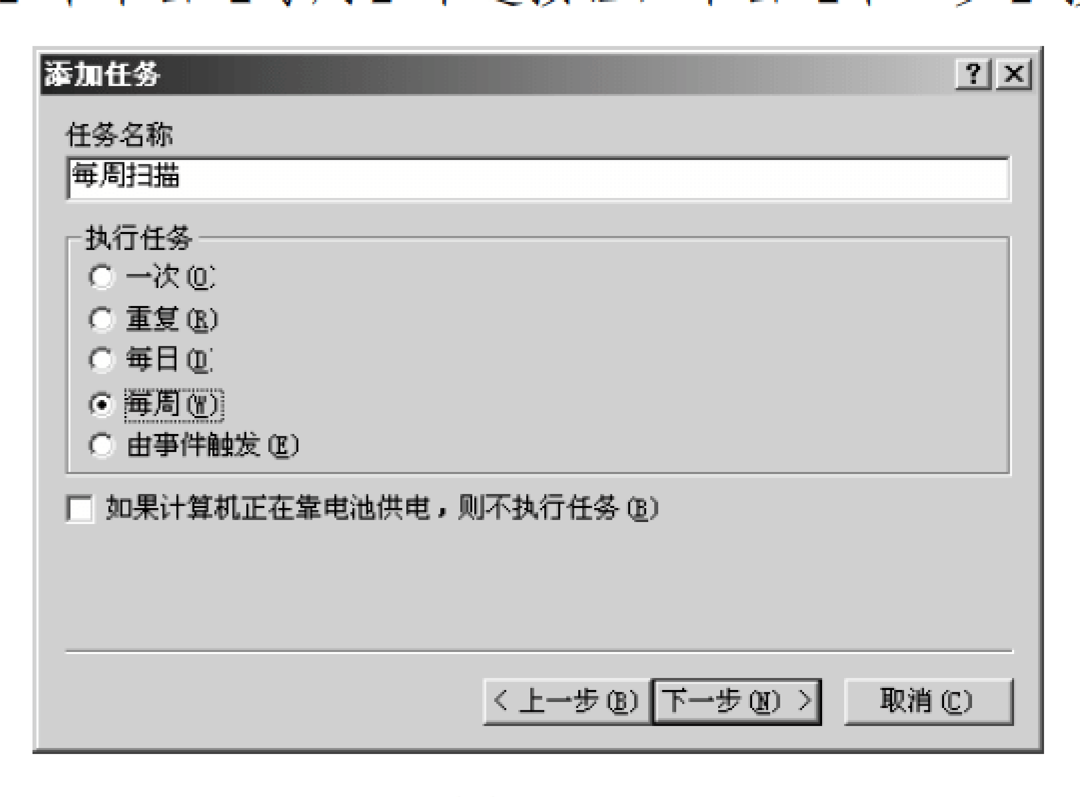


图 15-39

06 在弹出的对话框的【任务执行时间】文本框中指定时间为“8:00:00”，如图 15-40 所示，勾选【周一】复选框，每周一早晨 8 点执行任务，单击【下一步】按钮。



图 15-40

07 如果在预定的任务计划时间系统因关机等原因无法完成任务，应让系统在恢复正常后迅速执行计划任务，如图 15-41 所示，单击【尽快执行任务】单选按钮，单击【下一步】按钮。

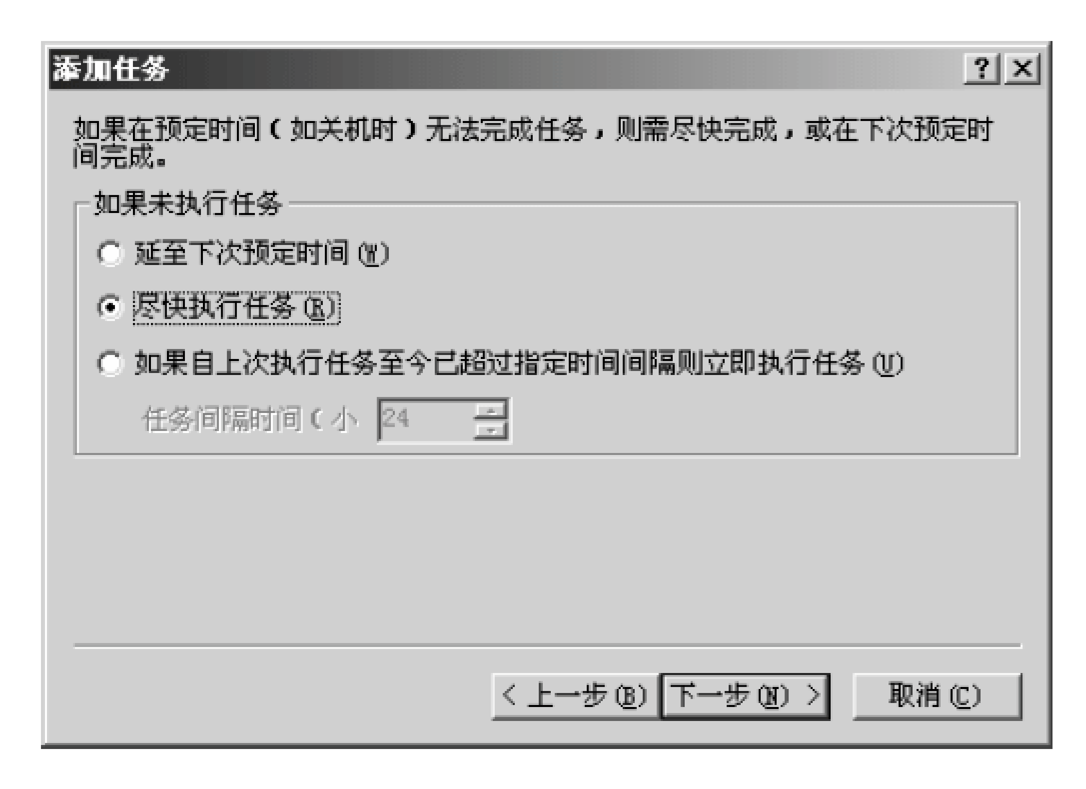


图 15-41

08 计划任务配置完成，在弹出的窗口中显示了计划任务的详细配置，单击【完成】按钮，如图 15-42 所示。



图 15-42

09 弹出【特殊设置】对话框，在【说明】文本框中输入关于本次计划任务的描述“每周扫描计算机”，选择【配置文件】选项，在【值】下拉菜单选项中选择计算机扫描采用的配置文件，本实例采用默认配置“全部扫描”，如图 15-43 所示。

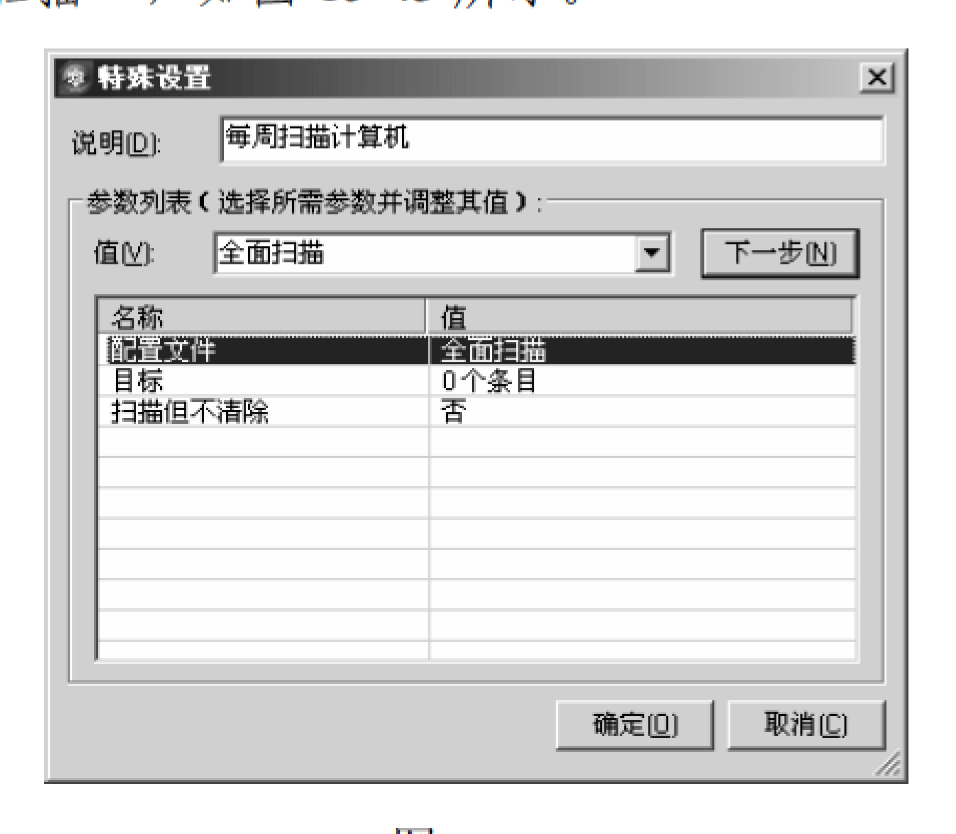


图 15-43

10 选择【目标】选项，单击【目标】按钮，指定扫描目标，如图 15-44 所示。



图 15-44

11 弹出【文件夹和文件】对话框，可以指定文件夹、文件、列表、驱动器和内存为扫描目标，本实例以驱动器为例进行介绍，单击【驱动器】按钮，如图 15-45 所示。

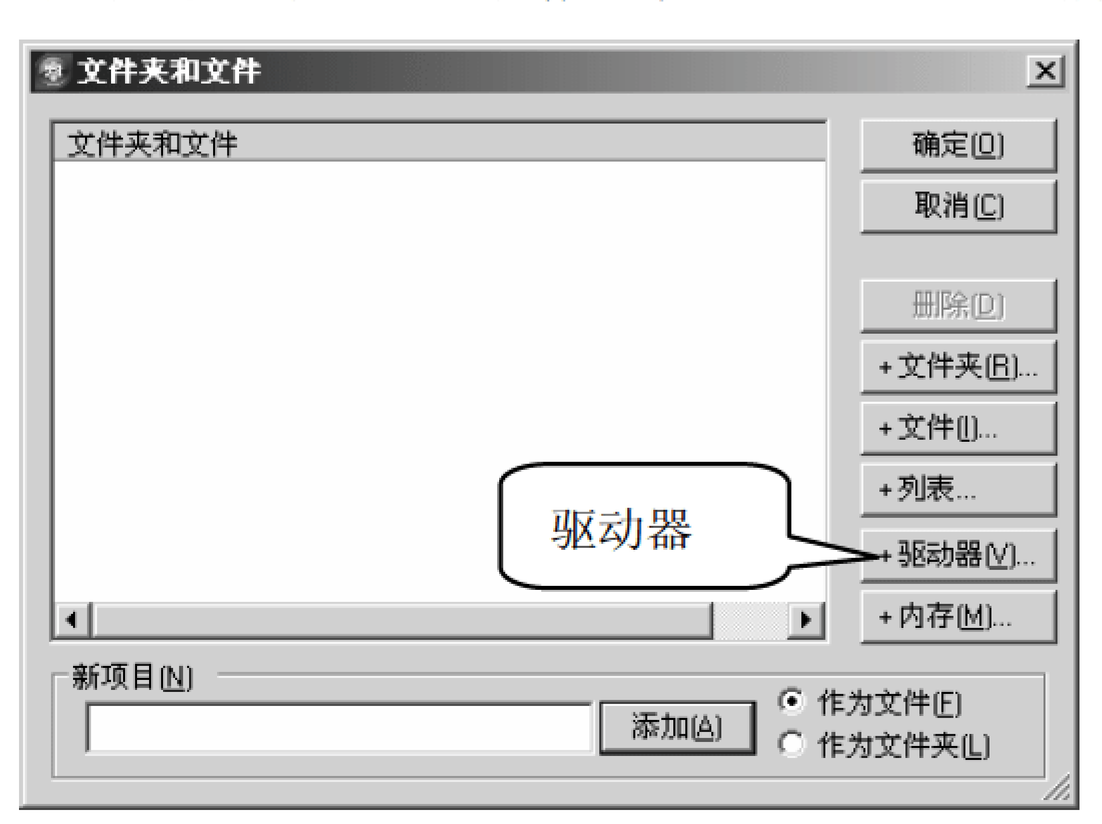


图 15-45

12 弹出【客户端扫描目标选择】对话框，可根据情况进行选择，为了安全建议勾选【所有驱动器】复选框，如图 15-46 所示，单击【确定】按钮。



图 15-46

13 返回【文件夹和文件】对话框，可继续添加其他目标，单击【确定】按钮，完成添加，如图 15-47 所示。



图 15-47

14 返回【特殊设置】对话框，【目标】选项后的【值】显示为【1 个条目】，如图 15-48 所示，单击【确定】按钮。



图 15-48

15 返回【计划任务】对话框，计划任务添加成功，并自动分配了任务 ID，如图 15-49 所示，可以单击【添加】按钮继续添加计划任务，添加完成后单击【确定】按钮。



图 15-49

16 返回【ESET 配置编辑器】窗口，如图 15-50 所示，可以看到“计划任务：总计 1/0”，表示当前已有一个计划任务添加成功。



图 15-50

3. 更新模块的设置

所有客户机在更新程序及病毒库时，必须要有统一的更新配置，其中最重要的就是更新服务器的配置。下面介绍更新模块的配置方法。

选择【更新模块】➢【配置文件】➢【设置】➢【更新服务器】选项，在右侧【值】文本框中输入客户机可用的更新服务器地址，一般为安装 ESET 管理服务器的主机，本实例采用“http://192.168.1.102:2221”，其他设置项可根据情况配置，如图 15-51 所示。



图 15-51

4. 保存配置编辑器

配置编辑器设置完成后，要妥善保存。保存配置的具体步骤如下。

01 单击【ESET 配置编辑器】工具栏的【💾】按钮，弹出【CfgEdit】对话框，如图 15-52 所示，单击【是】按钮。

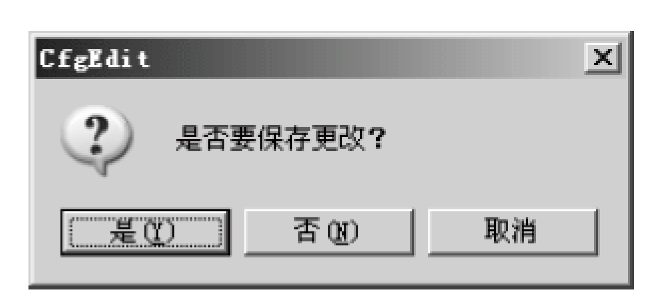


图 15-52

02 弹出【另存为】对话框，在【保存在】下拉菜单中选择合适的保存目录“我的文档”，

在【文件名】文本框中输入保存的文件名“config”，在【保存类型】下拉菜单选项中选择【配置文件（*.xml）】选项，如图 15-53 所示，单击【保存】按钮。

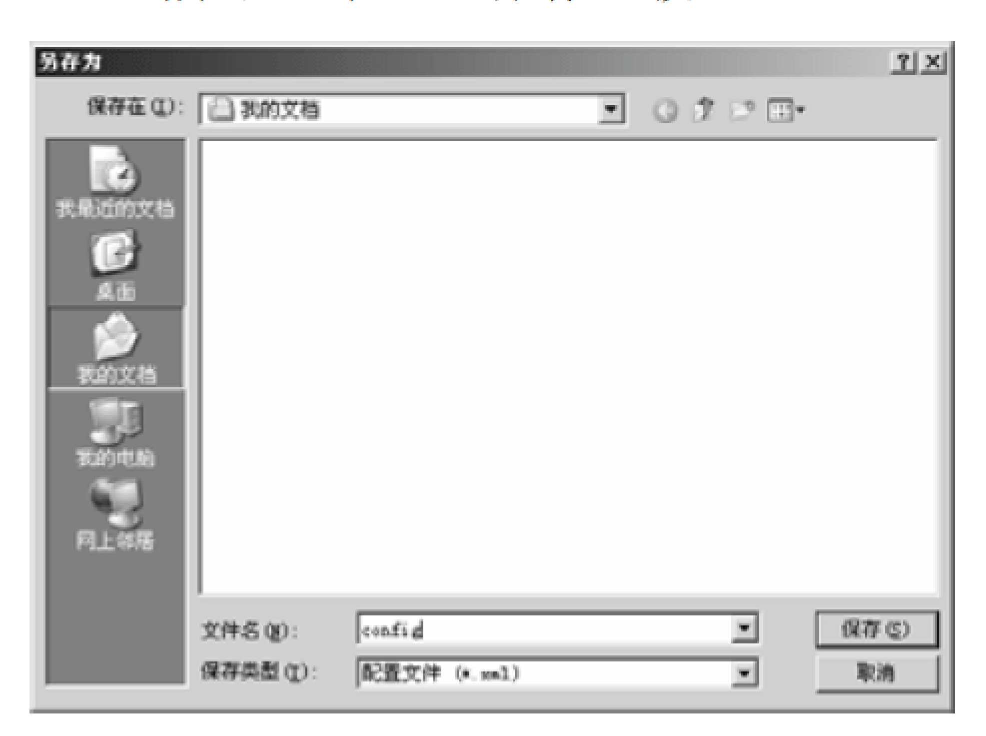


图 15-53



提 示

配置编辑器的其他内容，基本都可以不用去修改，系统已经默认设定好大部分的参数，这些默认配置可以最大限度地平衡计算机的性能。

15.2.3 设置客户端连接

客户端安装之后，需要被控制台统一管理，这需要在所有客户端配置连接管理控制服务器。设置客户端连接的具体操作步骤如下。

01 运行 ESET NOD32 客户端反病毒程序，打开程序主界面，选择左侧的【设置】选项，单击右侧的【切换到高级模式】超级链接，如图 15-54 所示。



图 15-54

02 弹出【切换到高级模式】提示对话框，单击【是】按钮，如图 15-55 所示。

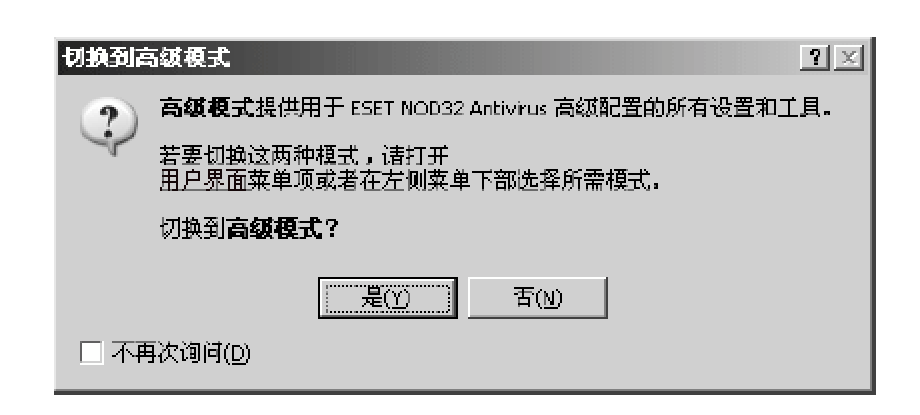


图 15-55

03 在右下方显示了更多配置项，单击【显示所有高级设置】超级链接，如图 15-56 所示。

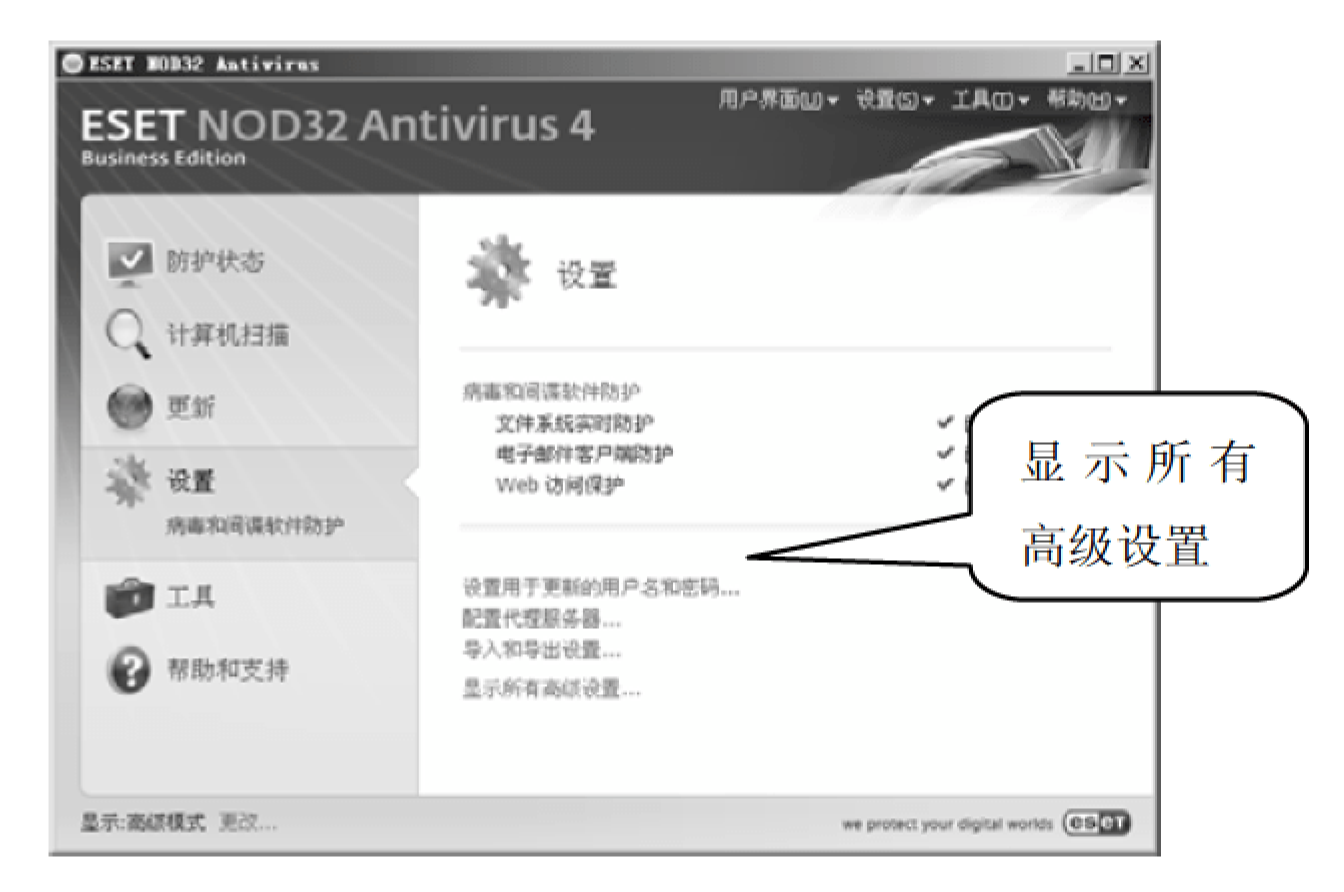


图 15-56

04 弹出【设置】对话框，选择左侧【更新】选项，在右侧【更新服务器】下拉菜单中选择更新程序及病毒库的服务器，默认使用【自动选择】，也可以单击【编辑】按钮，进行添加，如图 15-57 所示。

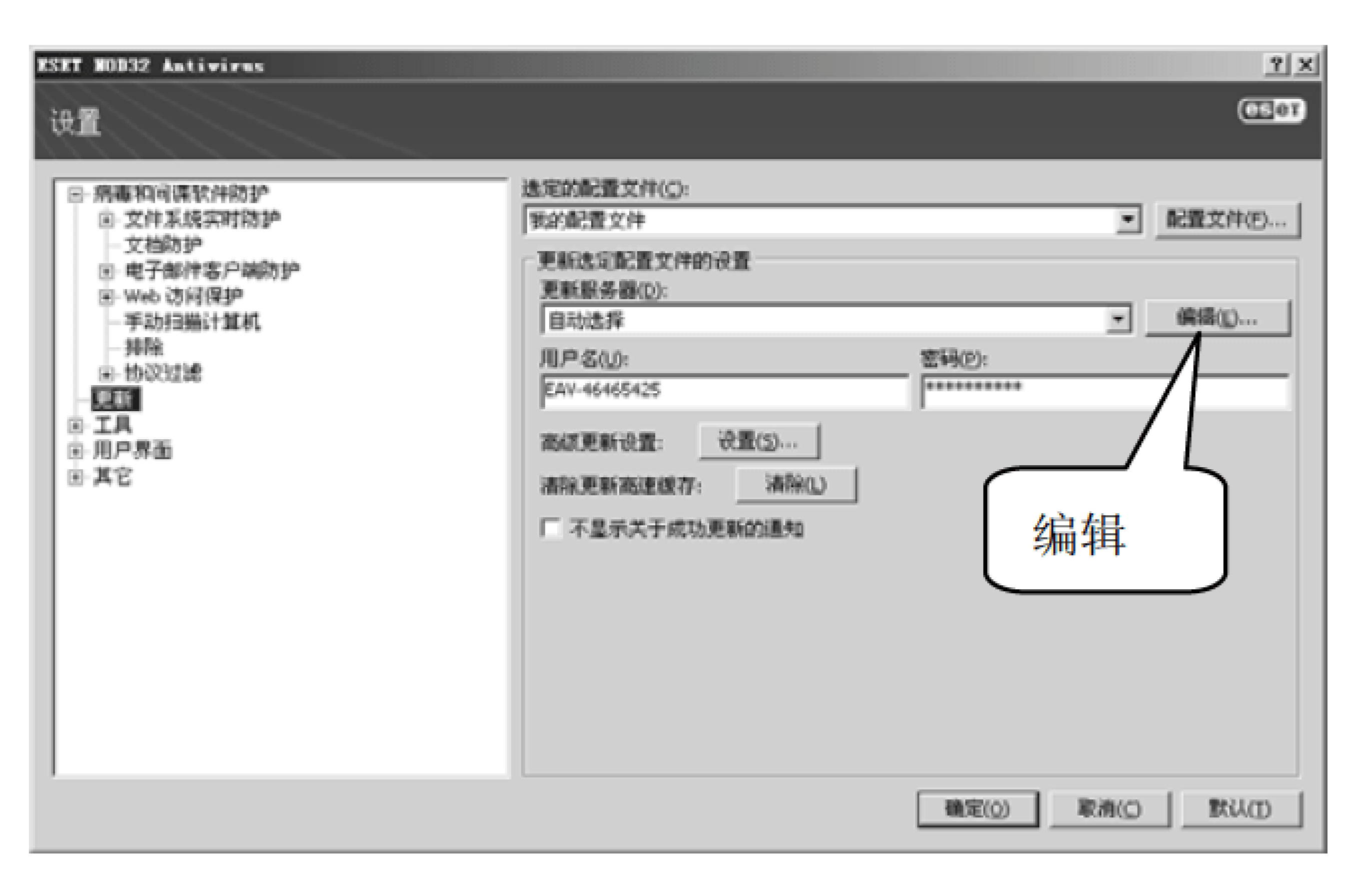


图 15-57

05 弹出【更新服务器列表】对话框，在【更新服务器】文本框中输入客户端可使用的更新服务器地址，该地址在管理服务器端有设置，本实例采用的是“http://192.168.1.102:2221”，单击【添加】按钮，如图 15-58 所示。



图 15-58

06 添加成功，如图 15-59 所示，在【更新服务器列表】中有添加后的地址，可以双击服务器地址直接修改，更新服务器地址正确添加后，单击【确定】按钮。



图 15-59

07 返回【设置】对话框，【更新服务器】下拉菜单选项的地址已经制定成功，如图 15-60 所示。

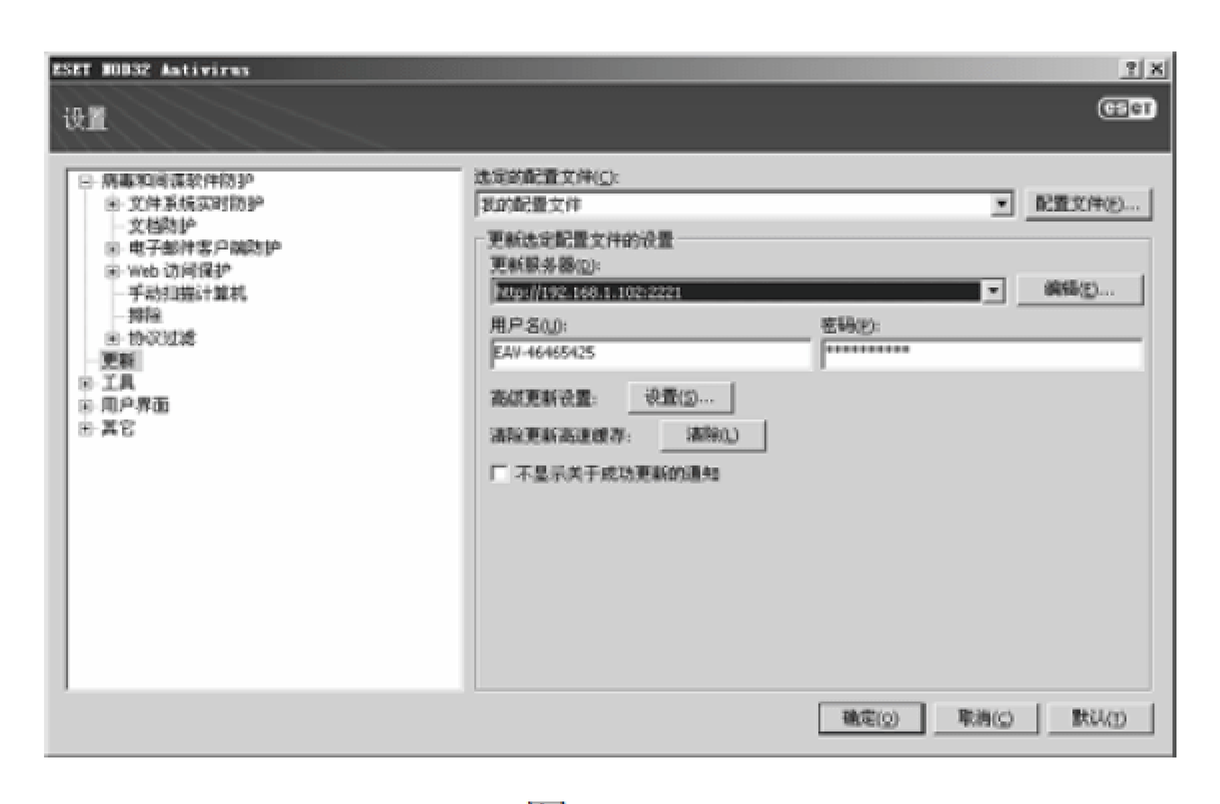


图 15-60

08 在左侧选项中选择【其它】➢【远程管理】选项，在右侧【服务器地址】文本框中输入安装管理服务器程序的主机 IP 地址，本实例采用“192.168.1.102”，在【端口】文本框中输入管理服务器指定的“2222”端口，单击【确定】按钮，完成客户端的配置，如图 15-61 所示。

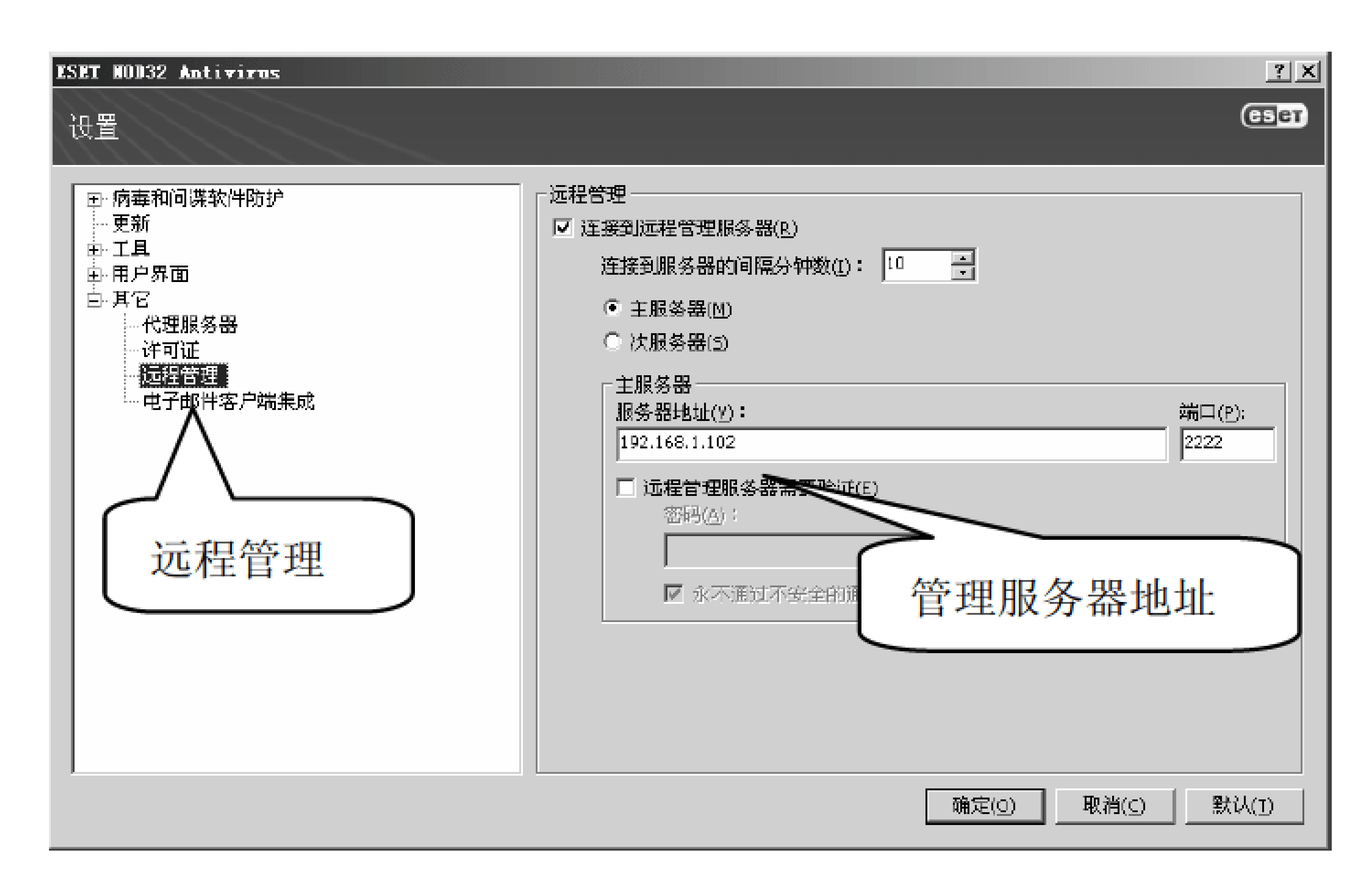


图 15-61

15.2.4　使用 ESET NOD32 进行全网杀毒

企业反病毒系统的环境做好之后，在日常管理中经常会遇到客户端感染病毒的现象，对此需要控制台对单个主机或全网进行病毒查杀。

在控制台进行全网病毒监控及查杀的具体操作步骤如下。

01 选择已有客户端，右击鼠标，在弹出的快捷菜单中选择【新任务】➢【手动扫描】菜单命令，如图 15-62 所示，根据需要，选择清除是否启用。

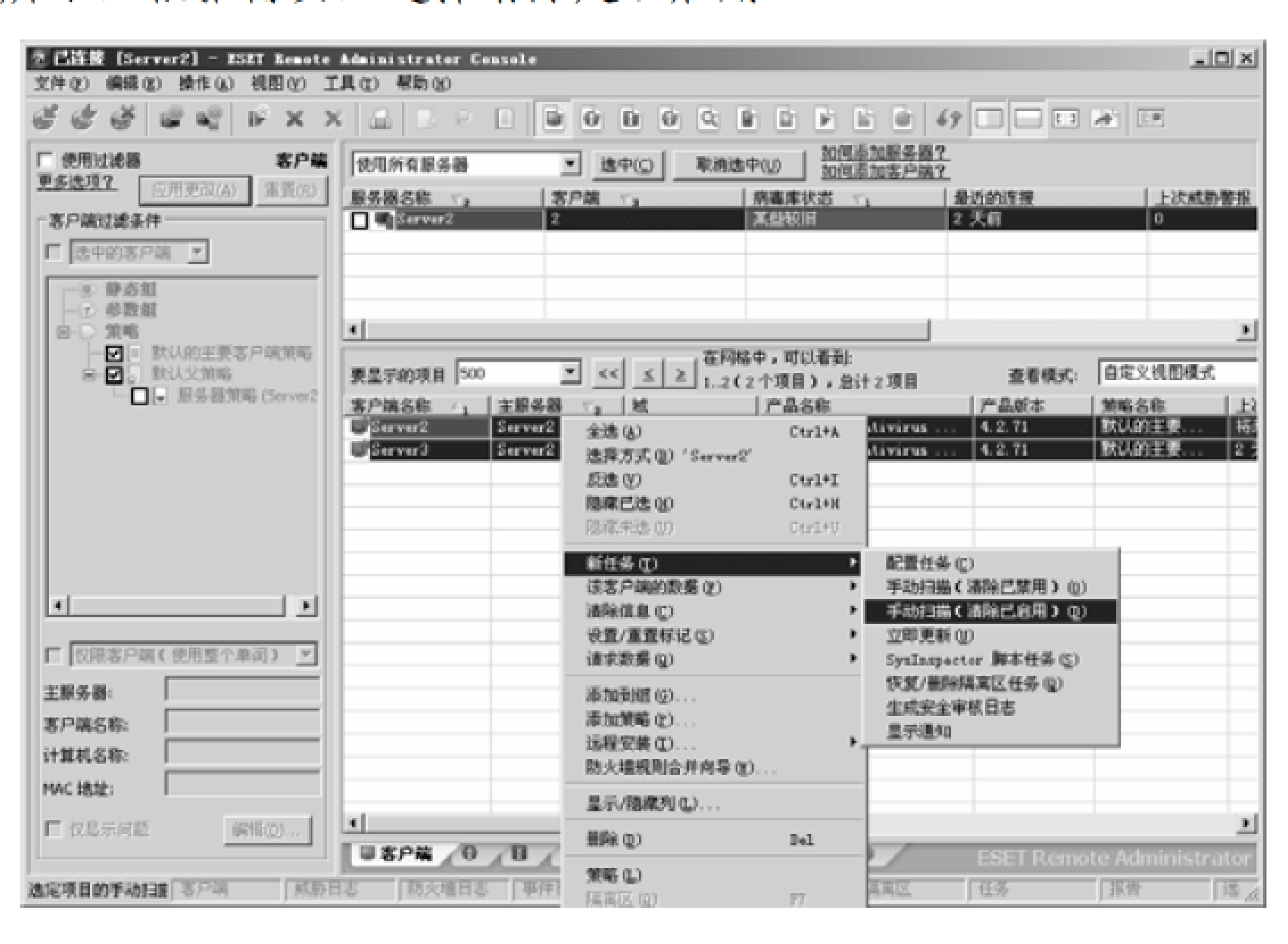


图 15-62

在【新任务】选项后有多个选项，主要选项介绍如下。

- 【配置任务】：用于配置计划任务，可不在此配置。
- 【手动扫描】：有两个选项，其差异在于扫描到病毒后的操作，【清除已禁用】表示扫描到的病毒只做提示不清除，而【清除已启用】会将扫描到的病毒直接清除。
- 【立即更新】：从图 15-62 可以看出，上方【病毒库状态】选项下有红色提示“某些较旧”，

可以通过【立即更新】选项解决病毒库或反病毒程序较旧的问题。

02 弹出【手动扫描】窗口，【配置部分】和【配置文件名】下拉菜单选项按默认配置，在【要扫描的驱动】选项框中，勾选需要扫描的项目，本实例采用默认配置，左下角的【扫描但不清除】复选框可根据情况选择，如图 15-63 所示，单击【下一步】按钮。



图 15-63

03 弹出【选择客户端】窗口，通过双击或者拖放的形式将左侧【所有项】列表中的服务器或客户端放入右侧【选定项目】列表中，单击【下一步】按钮，如图 15-64 所示。

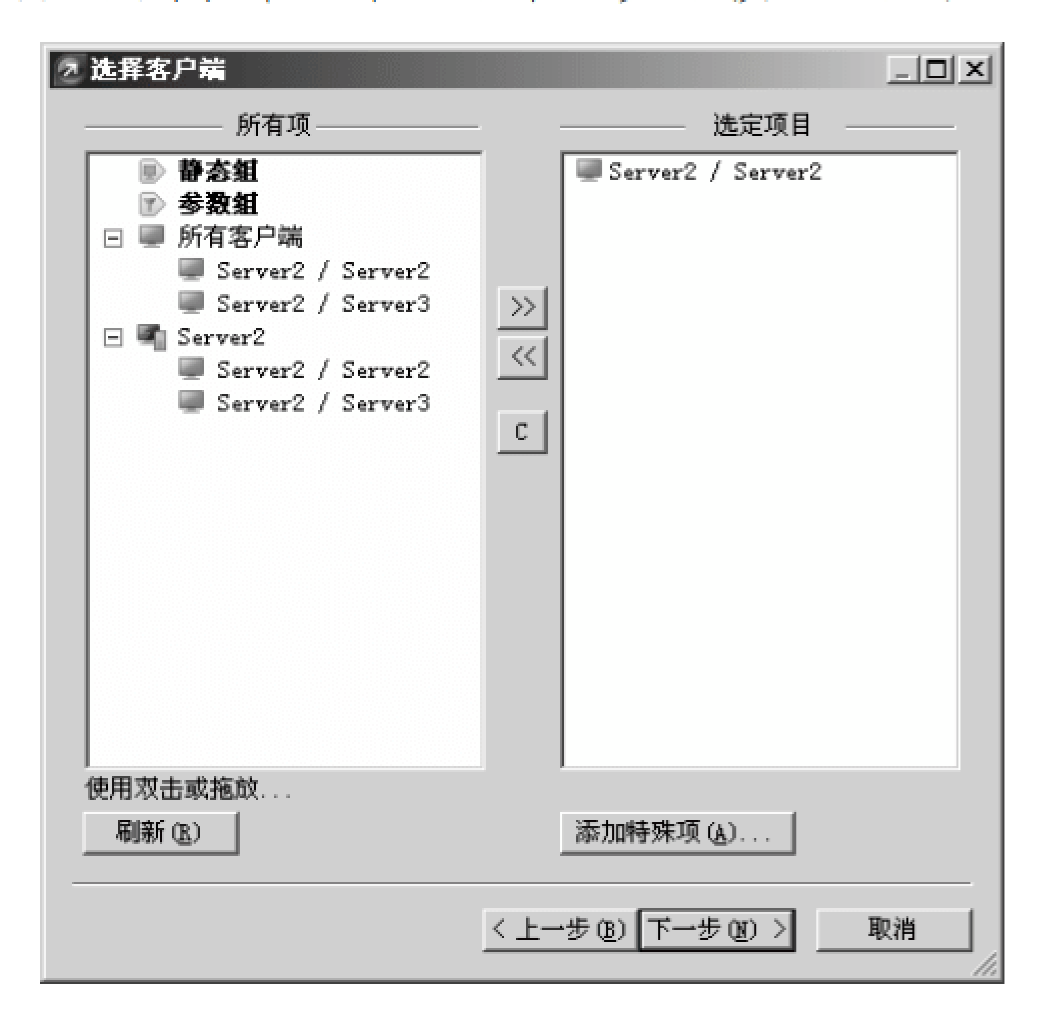


图 15-64

04 弹出【任务报告】窗口，在【新任务的最终报告】中显示新建扫描任务，在【任务设置】【名称】文本框中输入本次任务名，可以通过选择【该时间之后应用任务】复选框，设定定时扫描计划，本实例不做操作，为了方便排查故障，不建议选择【如果成功完成，则通过清除功能自动删除任务】复选框，单击【完成】按钮，开始客户端扫描，如图 15-65 所示。



图 15-65

15.3　项目实施 2：趋势科技企业反病毒系统实战案例

趋势科技是国内实力很强的反病毒系统，对于中国式病毒的防护具有比较显著的优势，下面详细介绍其环境架设及应用。

15.3.1　安装趋势科技企业反病毒系统

趋势科技反病毒系统对计算机内存要求稍高，最好使用 1G 以上内存。安装趋势科技反病毒系统的具体操作步骤如下。

01 运行趋势科技防毒墙网络版安装程序，弹出安装向导，单击【下一步】按钮，如图 15-66 所示。



图 15-66

02 弹出【许可证协议】对话框，选择【我接受许可证协议中的条款】单选按钮，如图 15-67 所示，单击【下一步】按钮。

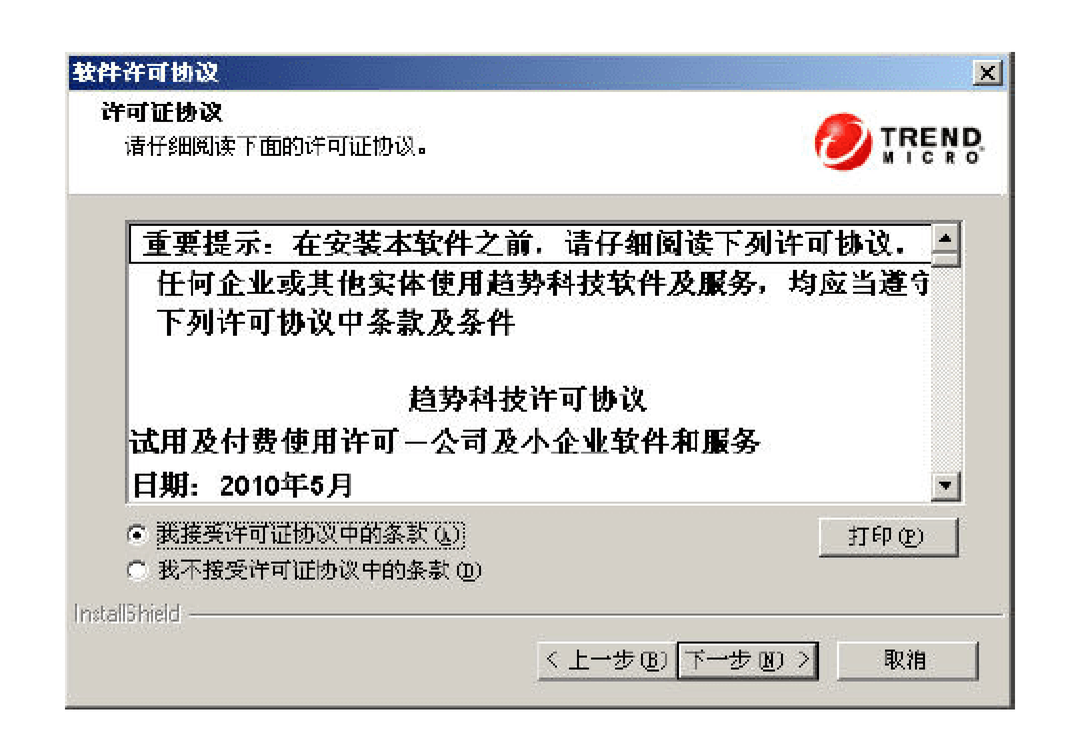


图 15-67

03 弹出【客户端部署】对话框，给出将客户端安装软件包部署到防毒墙网络版客户端所需的预估网络带宽，如图 15-68 所示，单击【下一步】按钮。



图 15-68

04 弹出【使用指南】对话框，如图 15-69 所示，提示安装前备份现有服务器配置，默认不操作，单击【下一步】按钮。

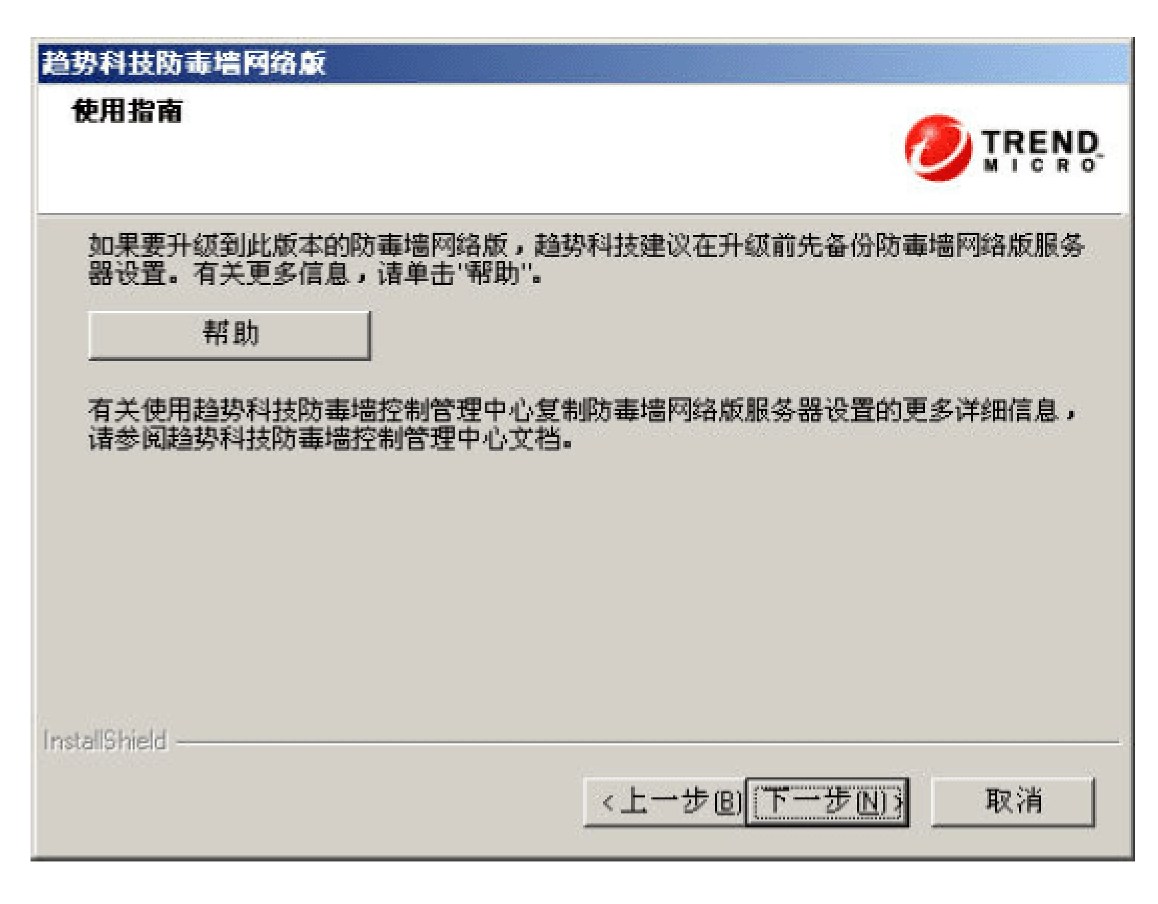


图 15-69

05 弹出【安装目标】对话框，选择【在此计算机上】单选按钮，如果需要将程序安装到远程主机，可以选择另一项，单击【下一步】按钮，如图 15-70 所示。



图 15-70

06 弹出【计算机预扫描】对话框，选择【扫描目标计算机】单选按钮，如图 15-71 所示，对本机进行安全风险扫描，单击【下一步】按钮。

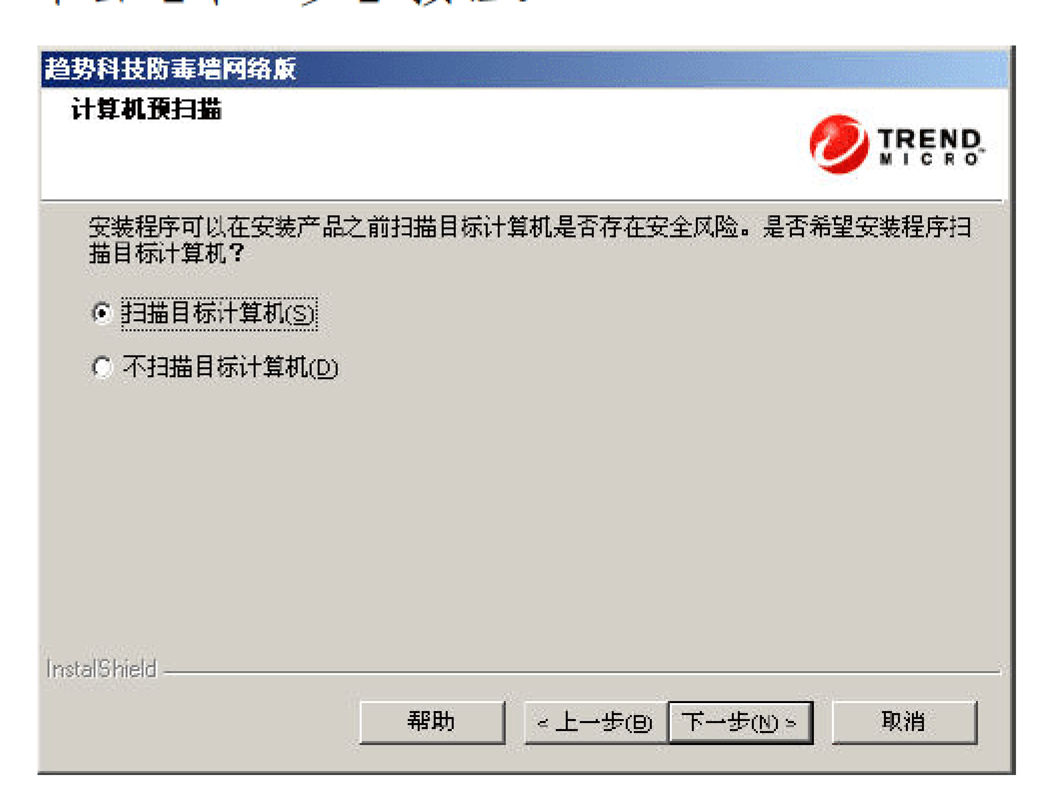


图 15-71

07 程序自动对目标操作系统进行扫描，并显示扫描进度，如图 15-72 所示。



图 15-72

08 扫描结束，弹出【安装路径】对话框，单击【浏览】按钮可以设定反病毒程序的安装路径，本实例采用默认配置，单击【下一步】按，如图 15-73 所示。



图 15-73

09 弹出【代理服务器】对话框，设定趋势科技企业反病毒程序访问 Internet 的代理服务器地址，本实例不做配置，单击【下一步】按钮，如图 15-74 所示。

图 15-74

10 弹出【Web 服务器】对话框，如图 15-75 所示，设置防毒墙服务器要使用的 Web 服务器，如果本机安装了 IIS 组件，可以选择【IIS 服务器】单选按钮，访问端口为 8080，如果本机没有安装 IIS 组件，只可以选择【Apache Web 服务器 2.0】单选按钮，使用 Apache 服务器安全性高于 IIS 服务器，本实例使用 IIS 服务器，单击【下一步】按钮。

图 15-75

11 弹出【计算机标识】对话框，可以设定防毒墙客户端识别服务器使用 IP 地址及域名，本实例采用默认配置【域名】单选按钮，文本框中显示为主机名，如图 15-76 所示，单击【下一步】按钮。

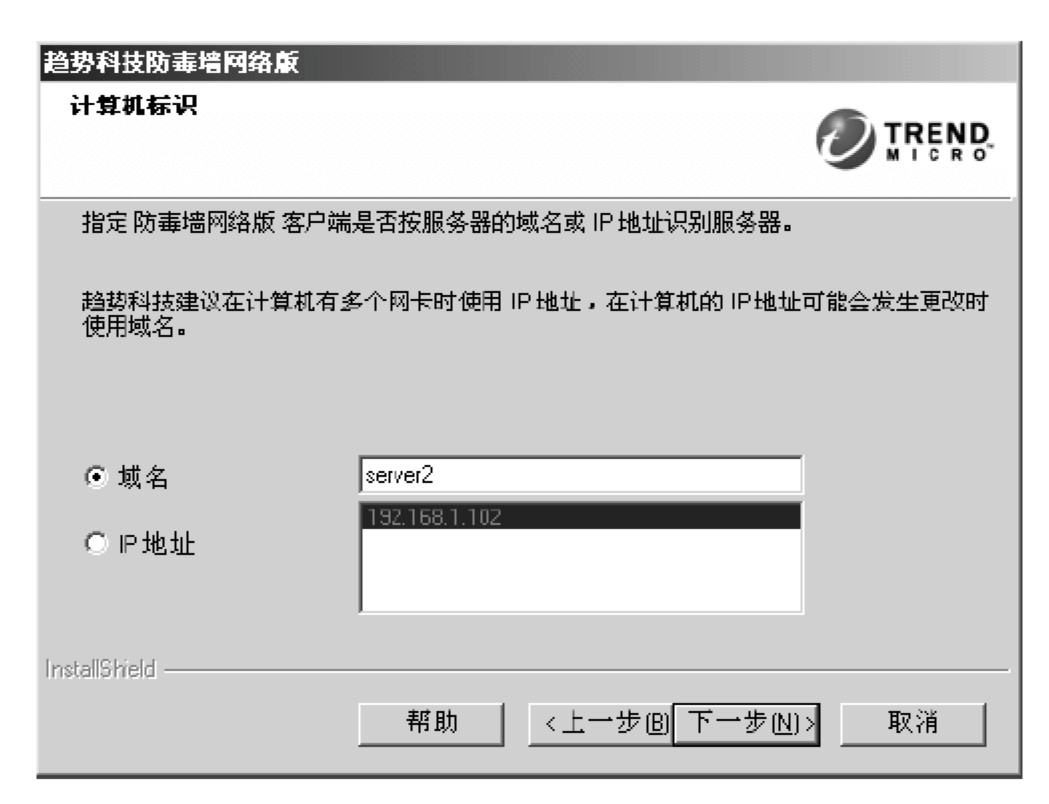


图 15-76

12 弹出【产品激活】对话框，如图 15-77 所示，单击【下一步】按钮。

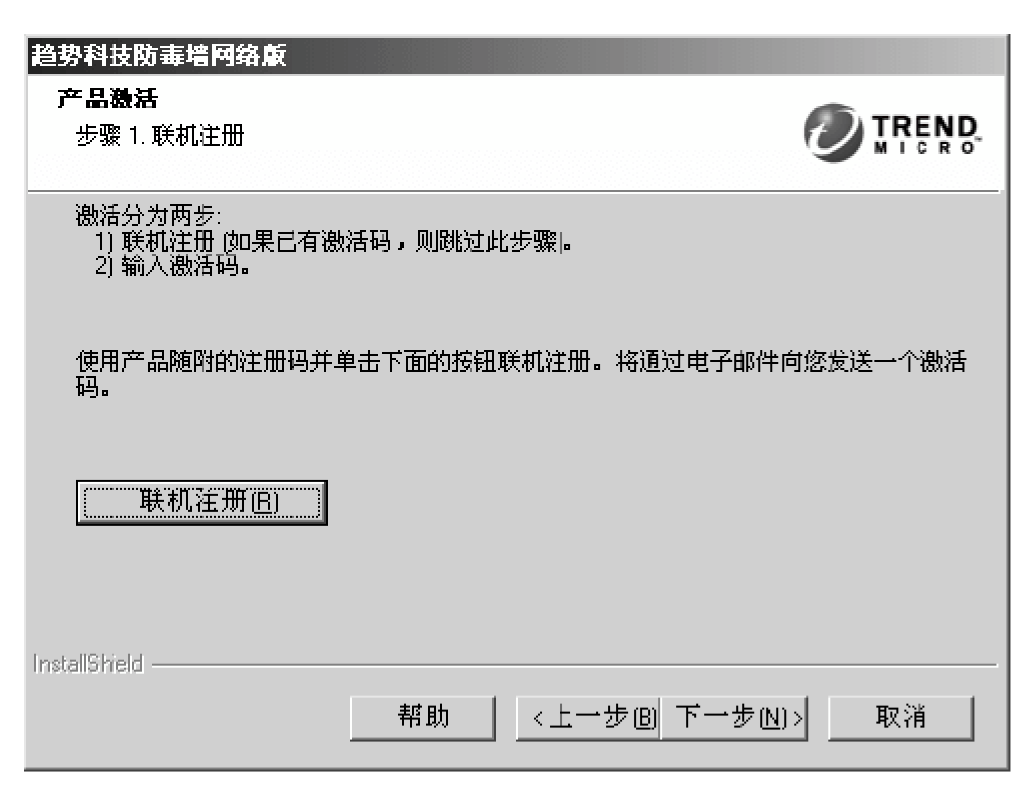


图 15-77

13 在【防病毒】、【损害清除服务】和【Web 信誉和防间谍软件】三个文本框中，分别输入已经获得的激活码，如图 15-78 所示，单击【下一步】按钮。

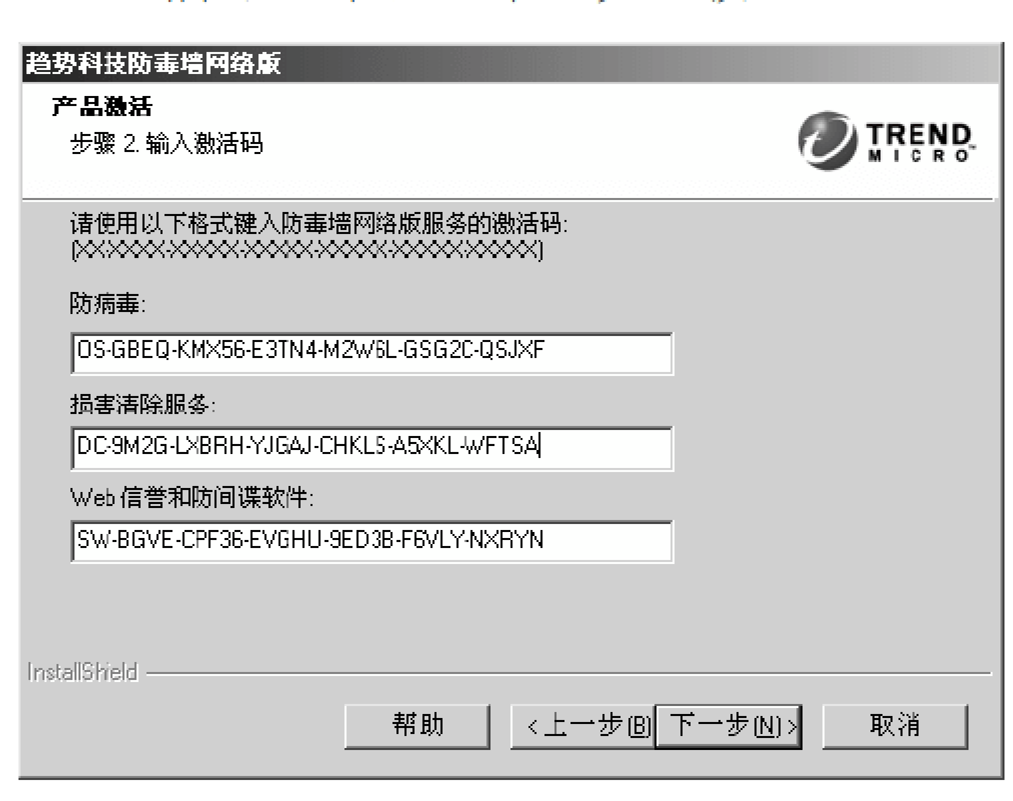


图 15-78

14 弹出【安装集成型云安全智能防护服务器】对话框，选择默认配置，如图 15-79 所示，单击【下一步】按钮。

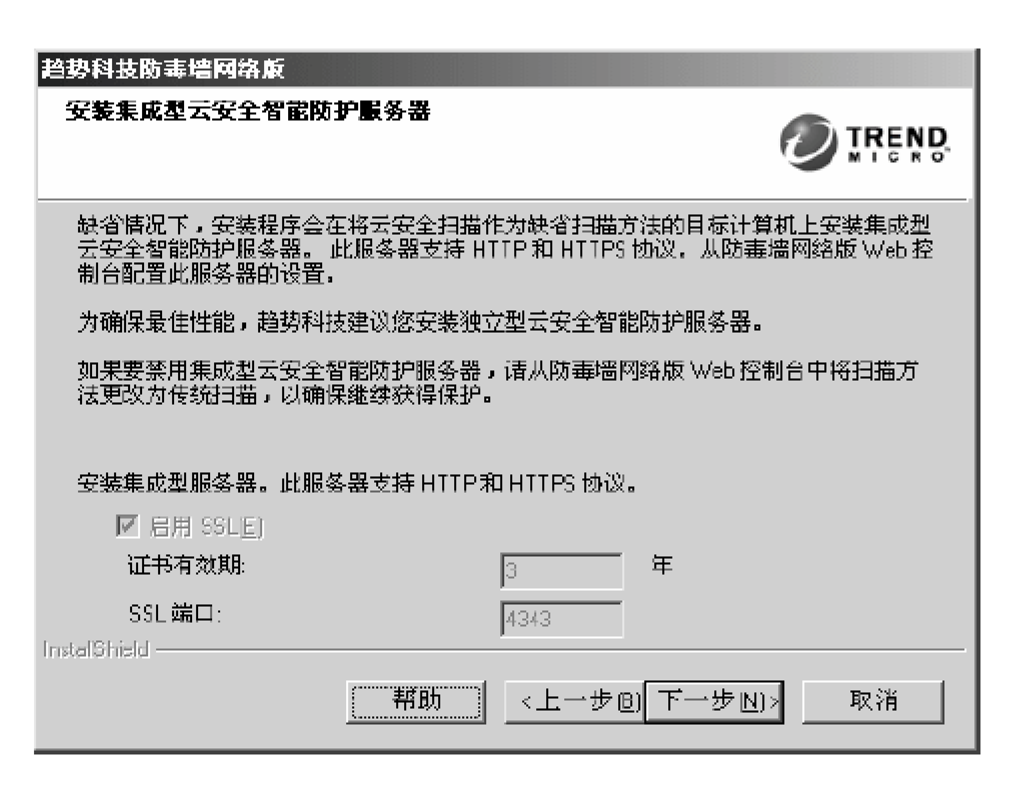


图 15-79

15 弹出【启用 Web 信誉服务】对话框，采用默认配置，如图 15-80 所示，单击【下一步】按钮。

图 15-80

16 弹出【安装其他防毒墙网络版程序】对话框，如图 15-81 所示，选择安装【防毒墙网络版客户端】程序，以确保防毒墙服务器使用客户端程序实施病毒防护（客户端程序可以实现病毒扫描、查杀），单击【下一步】按钮。

图 15-81

17 弹出【云安全智能防护网络】对话框，选择【启用趋势科技智能反馈】复选框，如图 15-82 所示，单击【下一步】按钮。



图 15-82

18 弹出【管理员账户密码】对话框，如图 15-83 所示，默认 Web 控制台访问账户为“root”，根据要求在制定文本框输入密码信息，建议【Web 控制台密码】和【客户端退出与卸载密码】的密码信息不要一样，单击【下一步】按钮。

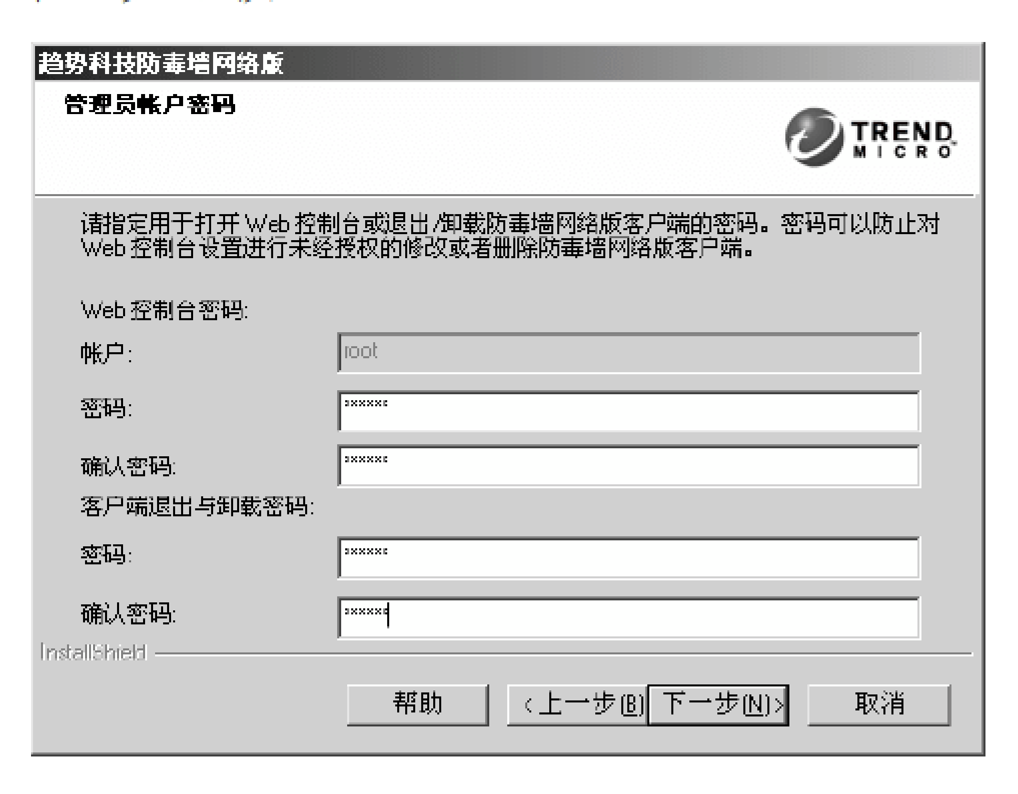


图 15-83

19 弹出【防毒墙网络版客户端安装】对话框，设置防毒墙客户端程序的默认安装路径、访问端口及安全级别信息，本实例采用默认配置，单击【下一步】按钮，如图 15-84 所示。

图 15-84

20 弹出【防病毒功能】对话框，如图 15-85 所示，选择【启用防火墙】复选框，以确保服务器的安全，单击【下一步】按钮。

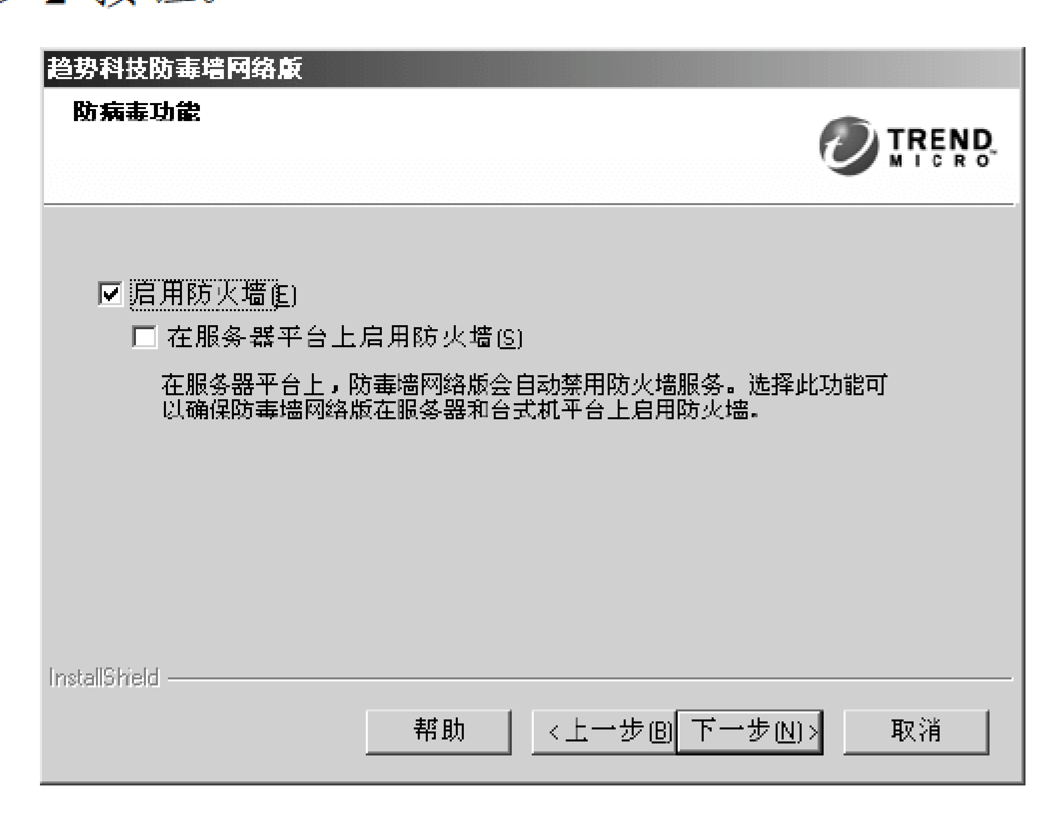


图 15-85

21 弹出【防间谍软件功能】对话框，选择【是，我想启用评估模式】单选按钮，如图 15-86 所示，以防护间谍软件和灰色软件的威胁，单击【下一步】按钮。

趋势科技防毒墙网络版
防间谍软件功能
评估模式设计为允许您先评估间谍软件/灰色软件是否合法，然后根据评估结果采取措施。单击"帮助"可获取详细信息。
是否要启用评估模式？
是，我想要启用评估模式(Y) 4 周
否，请不要启用评估模式(O)。
帮助 < 上一步(B) 下一步(N) > 取消

图 15-86

22 弹出【防毒墙网络版程序快捷方式】对话框，如图 15-87 所示，设定在【开始】中显示的程序名，采用默认配置，单击【下一步】按钮。

趋势科技防毒墙网络版
防毒墙网络版程序快捷方式
安装程序将在"开始"菜单中添加一个包含防毒墙网络版程序快捷方式的文件夹。请接受缺省文件夹名称或指定新文件夹名称。您也可以选择一个将在其中添加程序快捷方式的现有文件夹。
文件夹名称(F):
趋势科技防毒墙网络版服务器-SERVER2
现有文件夹:
HyperSnap 6
WinRAR
附件
管理工具
启动
< 上一步(B) 下一步(N) > 取消

图 15-87

23 弹出【安装信息】对话框，系统给出之前的配置摘要信息，单击【安装】按钮，如图 15-88 所示。

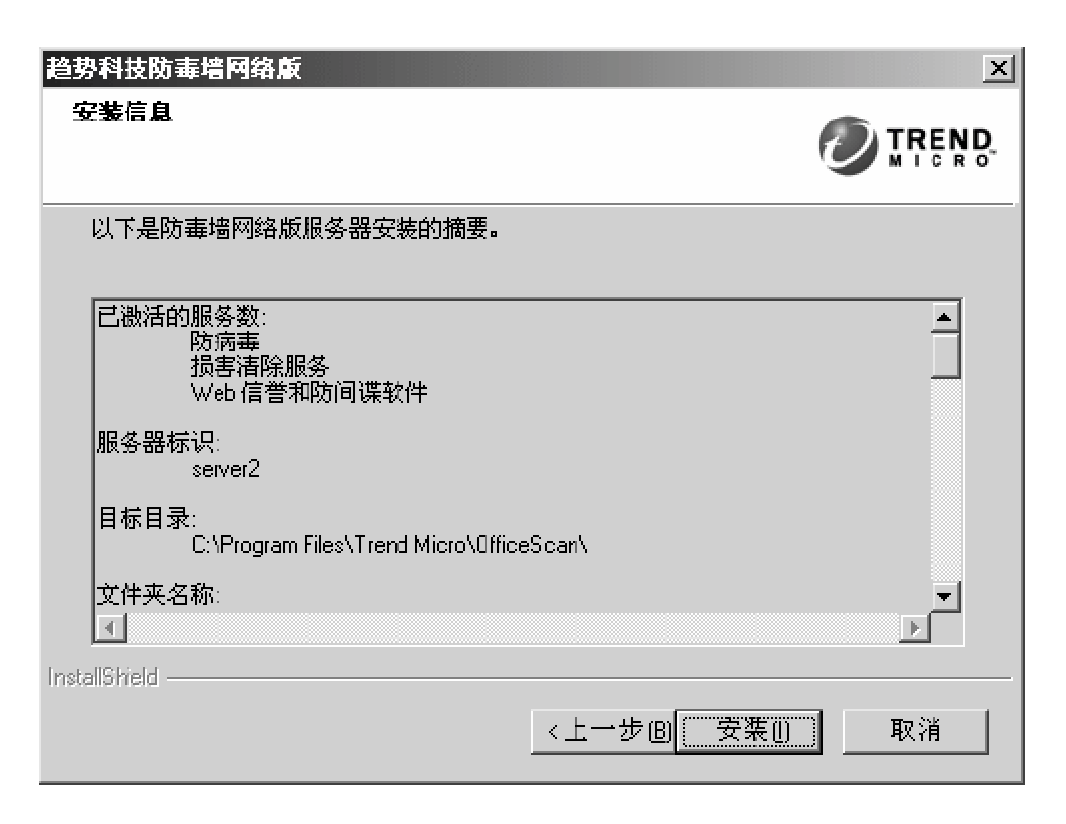


图 15-88

24 弹出【安装状态】对话框，系统依照配置自动安装程序，并显示安装进度，如图 15-89 所示。



图 15-89

25 弹出【安装完毕】对话框，可以根据需要选择【查看自述文件】和【打开 Web 控制台】复选框，单击【完成】按钮，完成趋势科技防毒墙的安装，如图 15-90 所示。

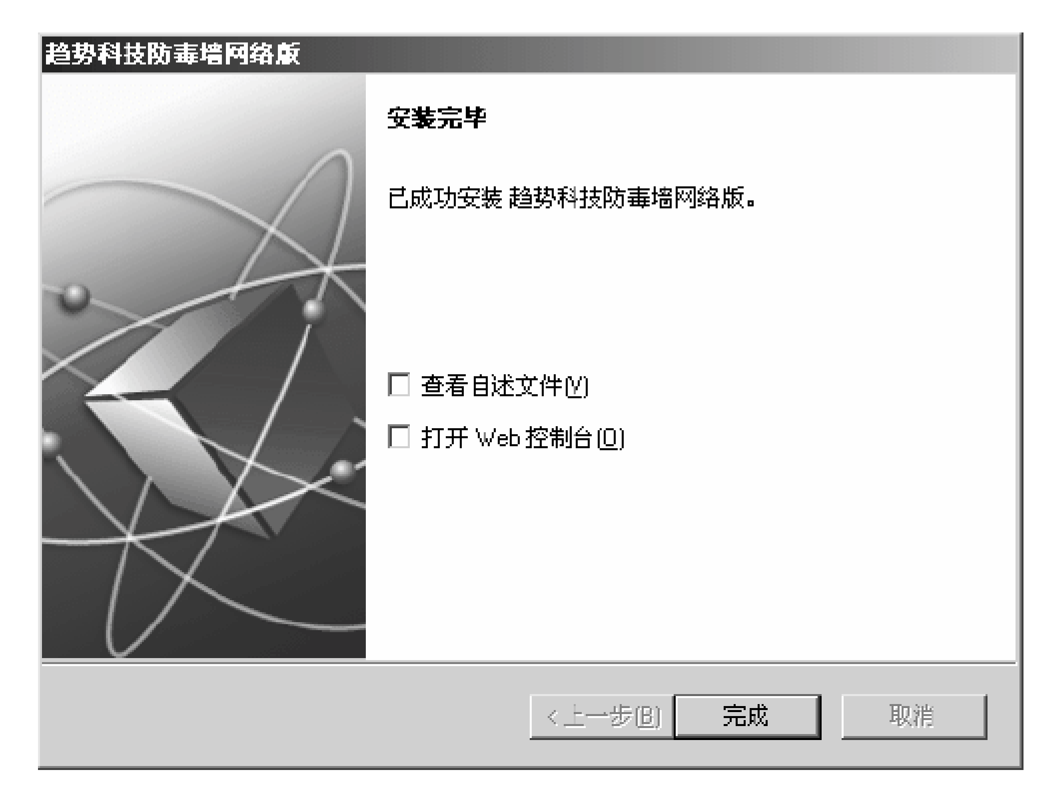


图 15-90

15.3.2 设置趋势科技软件防护内网安全

在使用趋势科技软件进行全网杀毒之前，需要设置趋势科技软件以防护内网安全。

1. 登录趋势科技 Web 控制台

01 选择【开始】➢【程序】➢【趋势科技防毒墙网络版服务器】➢【防毒墙网络版 Web 控制台（HTML）】菜单命令，如图 15-91 所示。



图 15-91

02 弹出【安全警报】对话框，单击【是】按钮，如图 15-92 所示。

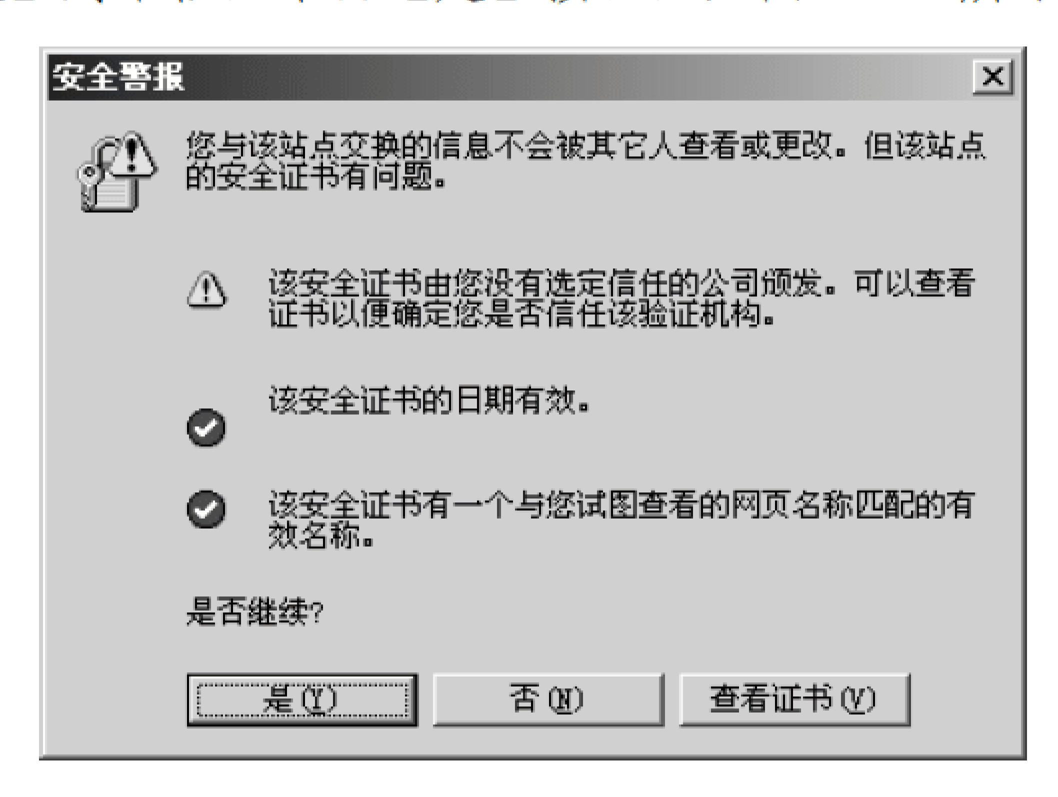


图 15-92

03 进入【WEB 控制台登录】页面，在【用户名】和【密码】文本框中分别输入有效信息，本实例采用默认账户“root”及安装时设定的密码“123123”，单击【登录】按钮，如图 15-93 所示。



图 15-93

04 进入趋势科技防毒墙网络版程序主页面，同时弹出【Internet Explorer-安全警报】对话框，提示安装程序必要组件，如图 15-94 所示，单击【安装】按钮。

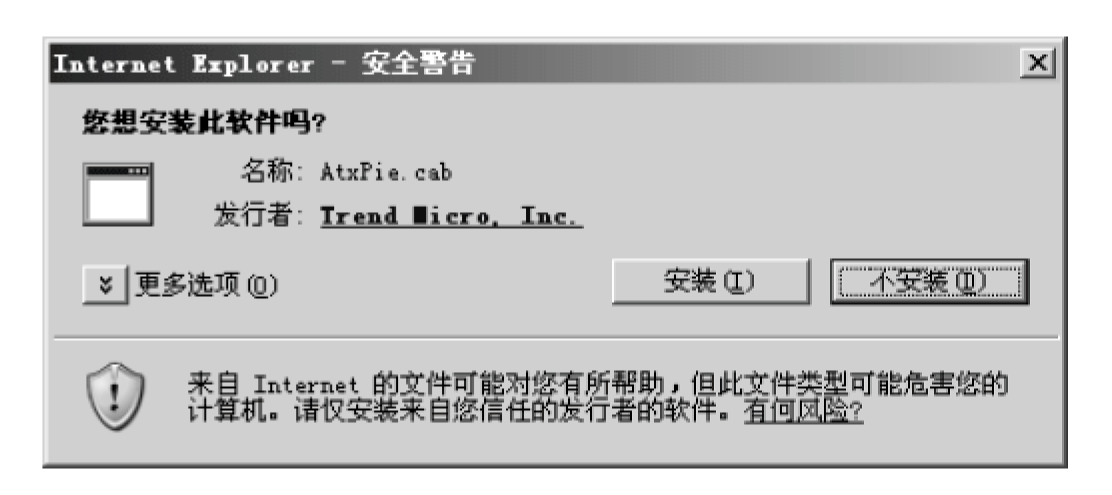


图 15-94

05 组件安装成功，显示程序主界面，默认显示【摘要】信息，包括客户端联机状态、病毒爆发状态、联网计算机更新状态等信息，如图 15-95 所示。



图 15-95

2．添加防毒墙客户端

想要对全网主机实施反病毒，必须将这些主机加入到反病毒系统中，因此，需要在所有主机

内安装防毒墙客户端程序。安装方法有两种，分别是：基于浏览器安装和远程安装。

（1）基于浏览器安装

具体的操作步骤如下。

01 在左侧选项列表中选择【联网计算机】➢【客户端安装】➢【基于浏览器】选项，在右侧界面的【电子邮件主题】文本框中设置客户端接收邮件的主题，本实例采用默认配置，单击【创建电子邮件】按钮，如图 15-96 所示。



图 15-96

02 在弹出的对话框中可以设置邮件信息，在【收件人】文本框中输入收件人邮箱地址，本实例使用 “user@163.com” 进行演示，其他采用默认配置，单击【发送】按钮，如图 15-97 所示。



图 15-97

03 本地没有发件人信息，所以首先要添加发件人，在弹出的【您的姓名】对话框中设置发件人显示名为 “user2” ，单击【下一步】按钮，如图 15-98 所示。



图 15-98

04 弹出【Internet 电子邮件地址】对话框，在【电子邮件地址】文本框中输入发件人邮箱地址，本实例使用“user2@163.com”，单击【下一步】按钮，如图 15-99 所示。



图 15-99

05 弹出【电子邮件服务器名】对话框，在【接收邮件服务器】和【发送邮件服务器】文本框中输入正确地址信息，由于本案例使用的是 163 邮箱，所以服务器使用如图 15-100 所示配置，单击【下一步】按钮。



图 15-100

06 弹出【Internet 邮件登录】对话框，在【账户名】文本框中输入“user2”，在【密码】文本框中输入指定邮箱的有效密码，单击【下一步】按钮，如图 15-101 所示。



图 15-101

07 弹出【祝贺您】对话框，如图 15-102 所示，邮件账户设置成功，单击【完成】按钮，向客户端发送邮件。



图 15-102



本实例中采用的邮箱地址及密码必须是当前网络的有效地址。

（2）远程安装

使用这种方法必须要有访问客户机的权限，以及有效的计算机账户和密码。远程安装的具体操作步骤如下。

01 在左侧选项列表中选择【联网计算机】➢【客户端安装】➢【远程】选项，右侧显示【远程安装】窗格。如图 15-103 所示，在【计算机名称】文本框中输入需要安装防毒墙客户端的客户机名称或 IP 地址，本实例以“192.168.1.103”主机为例进行讲解，单击【搜索】按钮。

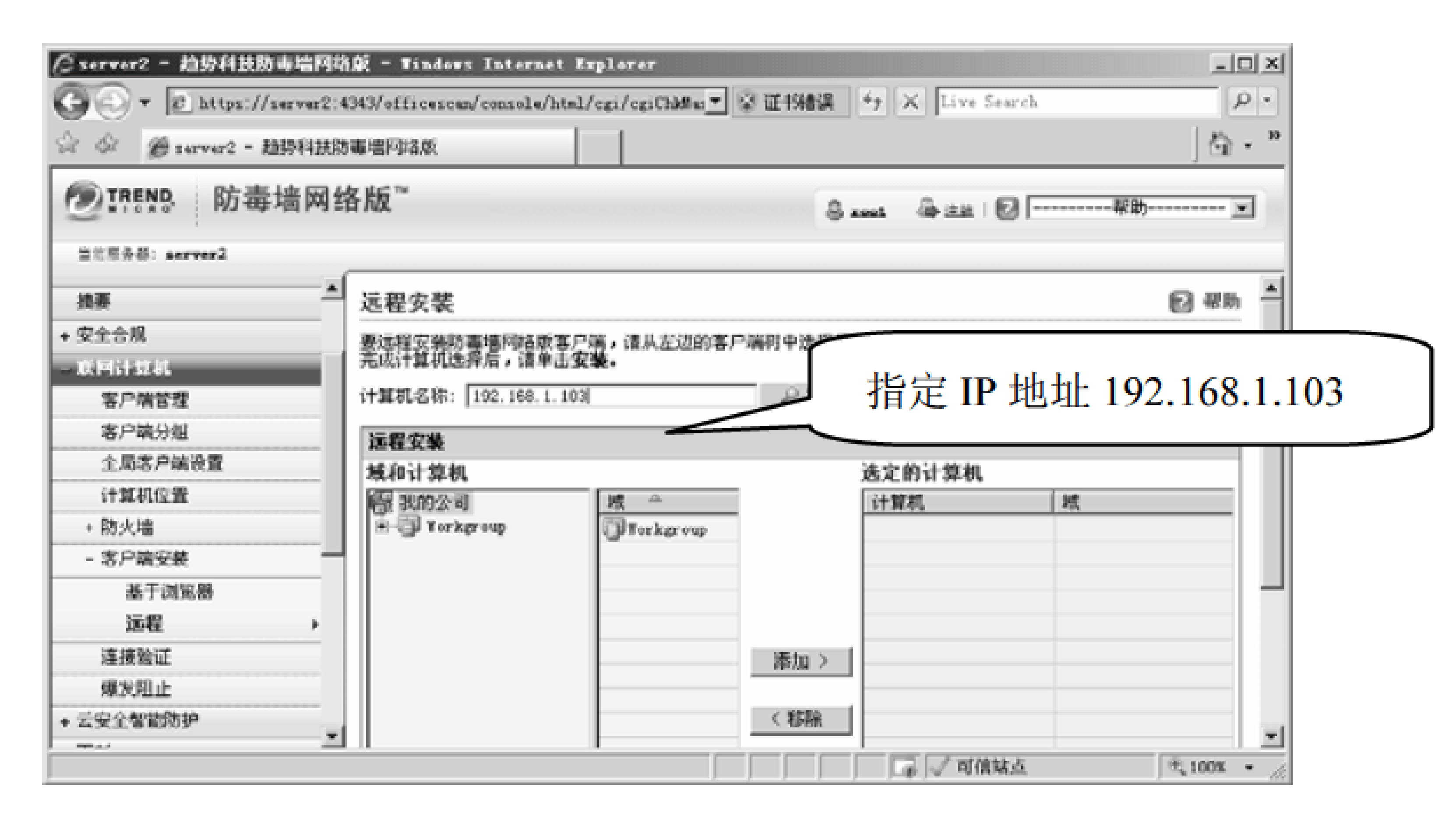


图 15-103

02 在弹出的对话框的【用户名】和【密码】文本框中，分别输入指定客户机的认证信息，如图 15-104 所示，单击【登录】按钮。



图 15-104

03 登录成功，在右侧的【选定的计算机】列表中显示了已连接成功的计算机，单击窗格左下侧的【安装】按钮，如图 15-105 所示。

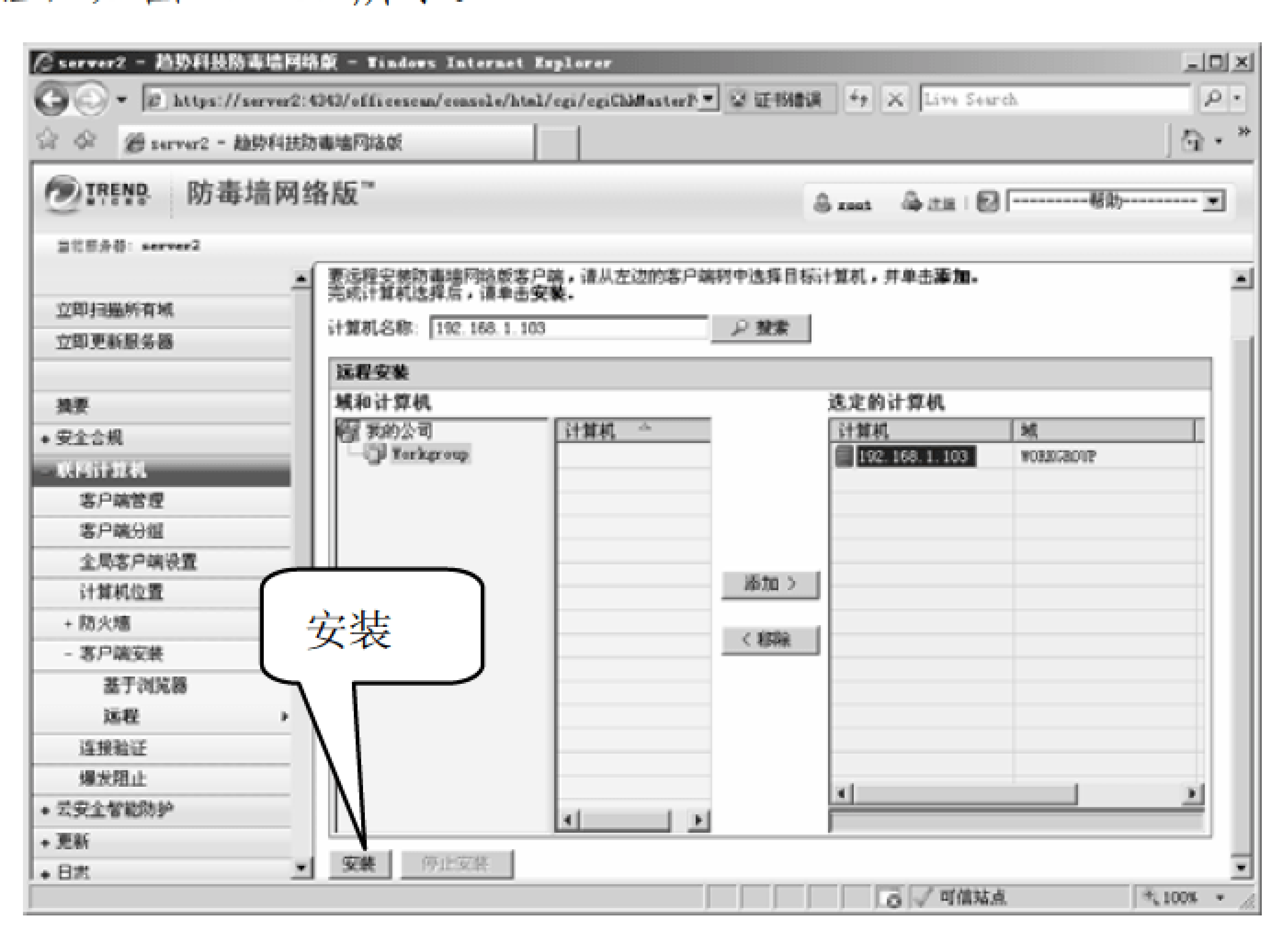


图 15-105

04 弹出【趋势科技防毒墙网络版管理控制台】对话框，如图 15-106 所示，提醒是否在指定的“192.168.1.103”计算机上安装客户端程序，单击【是】按钮。

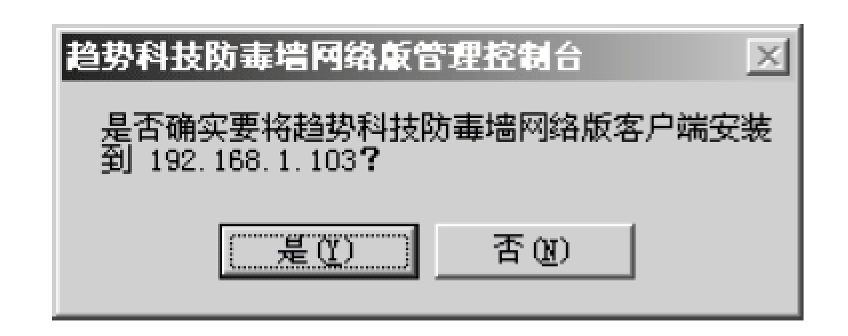


图 15-106

05 自动安装客户端程序，安装成功后显示如图 15-107 所示对话框，单击【确定】按钮。

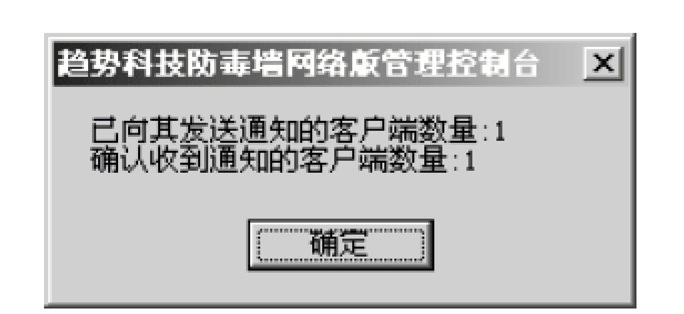


图 15-107

06 返回程序控制台页面，在右侧【选定的计算机】列表中，“192.168.1.103”计算机图标被勾选，如图 15-108 所示。

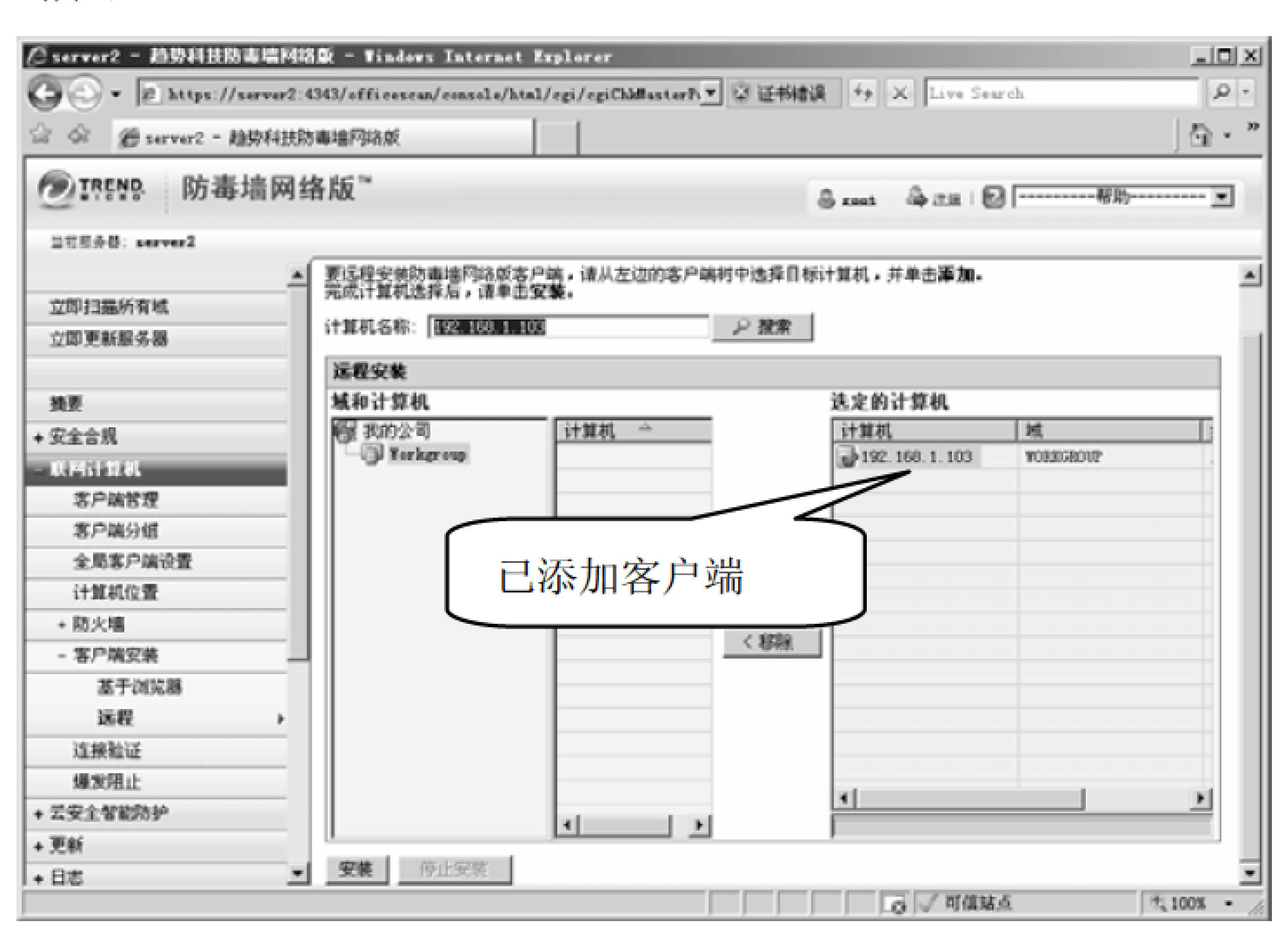


图 15-108

以上方法每次只能连接一个客户机，想要同时连接多个客户机时，可以使用如下操作方法完成。

在如图 15-108 所示的【域和计算机】窗格中显示了系统自动扫描到的工作组网络中的计算机信息，选中需要添加的计算机，单击【添加】按钮，可将其加入到右侧【选定的计算机】窗格中，被选定的计算机可以通过单击【安装】按钮完成客户端安装。

3. 管理客户端

防毒墙客户端安装完成后，需要对这些客户端进行管理。管理客户端的具体操作步骤如下。

01 在左侧列表中选择【联网计算机】➢【客户端管理】选项，展开右侧【客户端管理】页面，该页面可以显示出客户端计算机列表，也可以对指定的计算机进行管理操作，如图 15-109 所示。



图 15-109

02 选中一个客户机，单击【状态】按钮，进入状态设置界面，如图 15-110 所示。

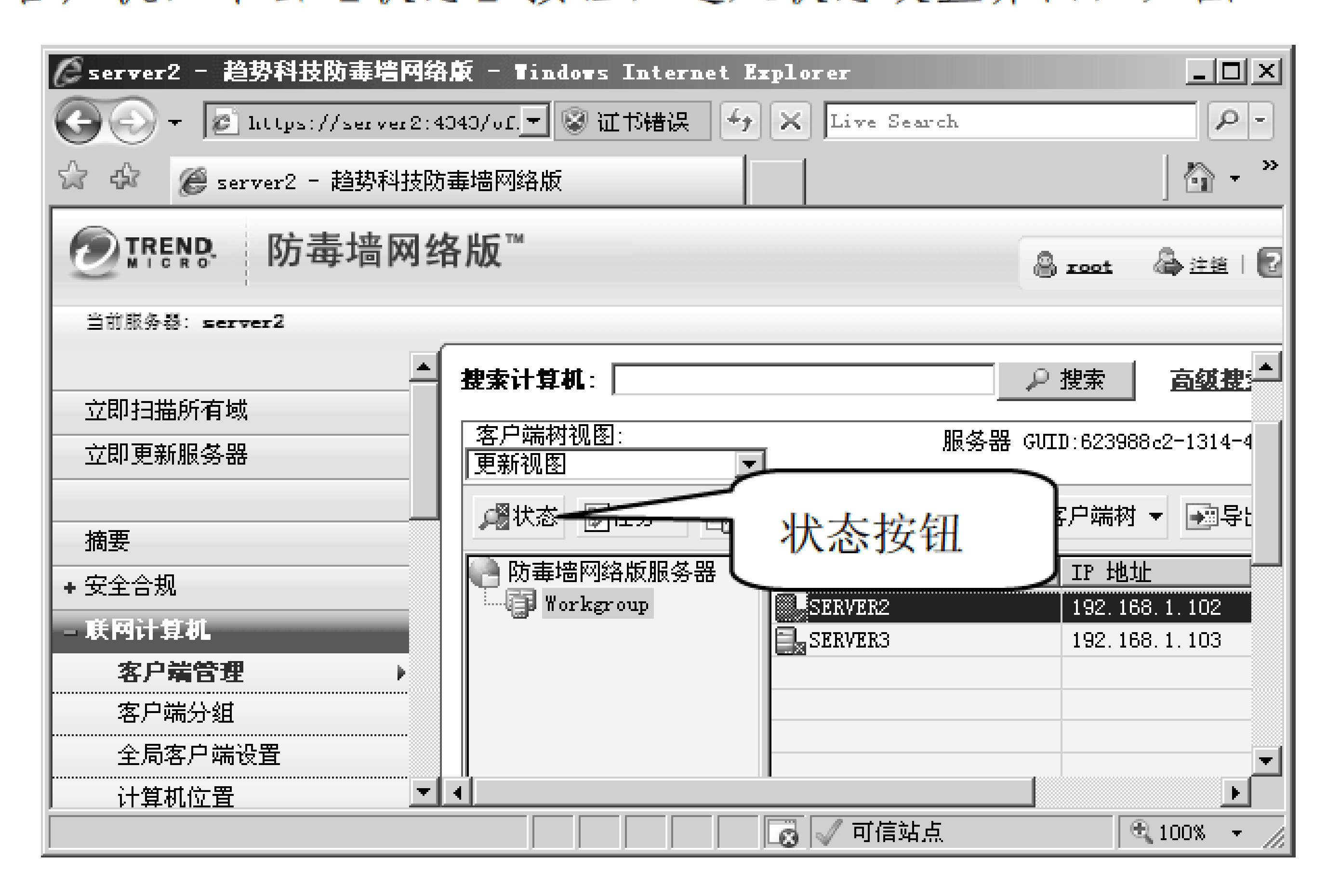


图 15-110

03 选中一个或多个客户机，单击【任务】按钮，弹出其下拉列表，可以对选中的客户机执行三种操作，分别是【立即扫描】、【客户端卸载】和【间谍软件/灰色软件恢复】，如图 15-111 所示。



图 15-111

04 单击【设置】按钮，弹出其下拉列表，可对客户机实施多种设置内容，如图 15-112 所示。

图 15-112

各个下拉列表选项的含义如下。

（1）扫描方法

对客户端进行扫描的方法有两种：【传统扫描】和【云安全扫描】，考虑到安全时效问题，一般建议选择【云安全扫描】。如果依靠本地存储的病毒库，往往会因为更新不及时，导致有新病毒出现时不能及时防御威胁。而云端存储的病毒库因有互联网提供新病毒资源，更新会快很多。但是如果网络环境不是很稳定，为了避免扫描失败也可以选择【传统扫描】，如图 15-113 所示。

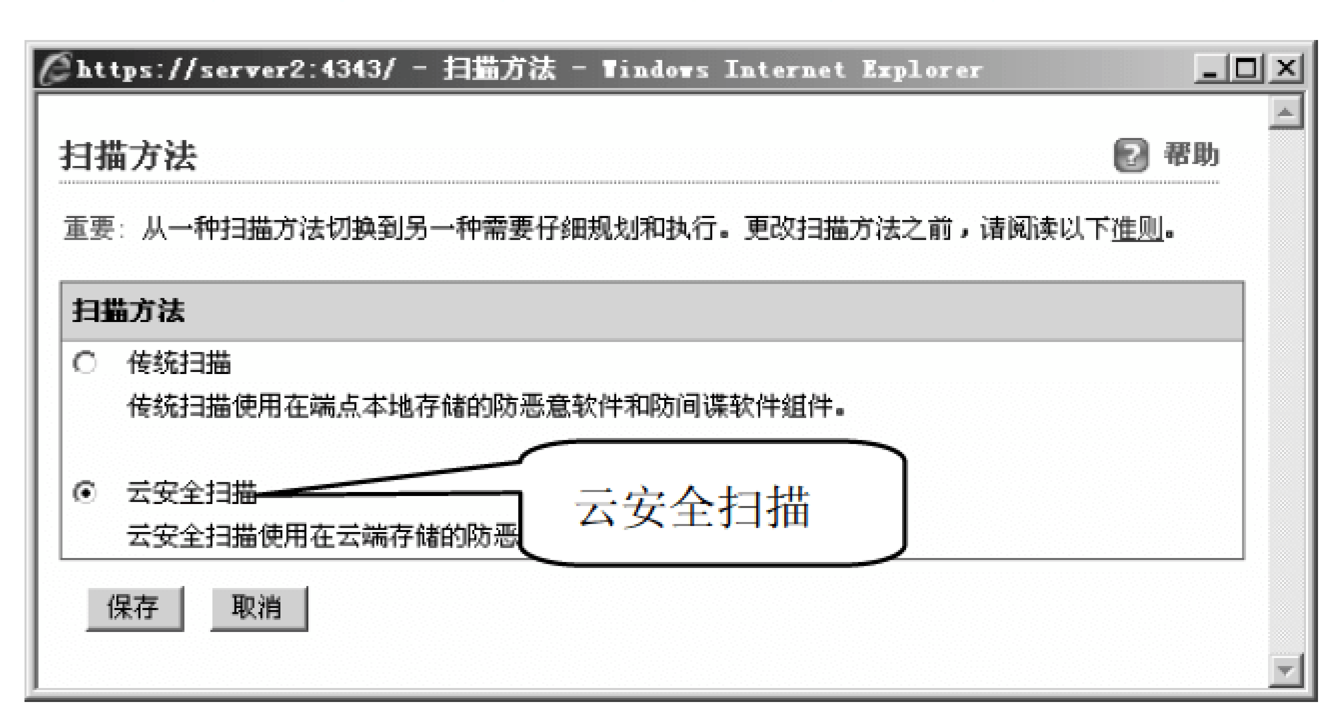


图 15-113

（2）手动扫描设置

当发现威胁时，管理员可以手动进行病毒扫描。管理员手动扫描时，使用本项配置。主要分为两部分：【目标】和【处理措施】，下面分别做介绍。

如图 15-114 所示，【目标】主要用于确定扫描对象。【要扫描的文件】选项用于指定需要扫描的文件类型，默认选择【IntelliScan】单选按钮。【扫描设置】选项用于指定特殊扫描设置，比如压缩文件的扫描深度、是否扫描隐藏文件等。



图 15-114

如图 15-115 所示，【处理措施】用于确定如何处理扫描出的病毒、木马。可根据需求进行配置，一般选择默认值。

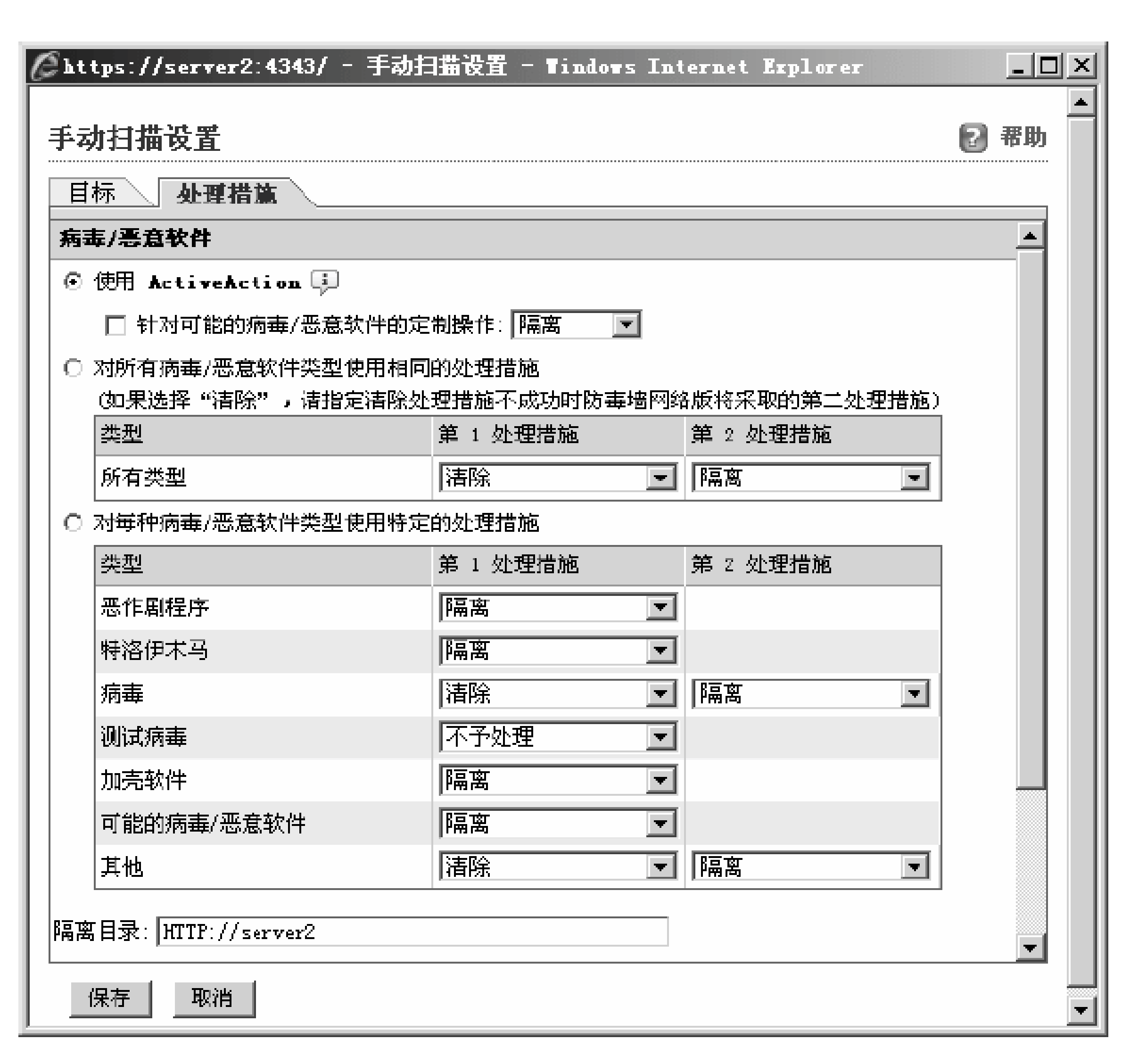


图 15-115

（3）实时扫描设置

日常应用中，反病毒程序会实时监控网络状态，防止病毒、木马攻击。实时监控网络安全状态的扫描采用如图 15-116 所示设置。



图 15-116

（4）预设扫描设置

为了安全，经常会设置一些定时的扫描任务，这类任务称作预设扫描任务，采用如图 15-117 所示设置。

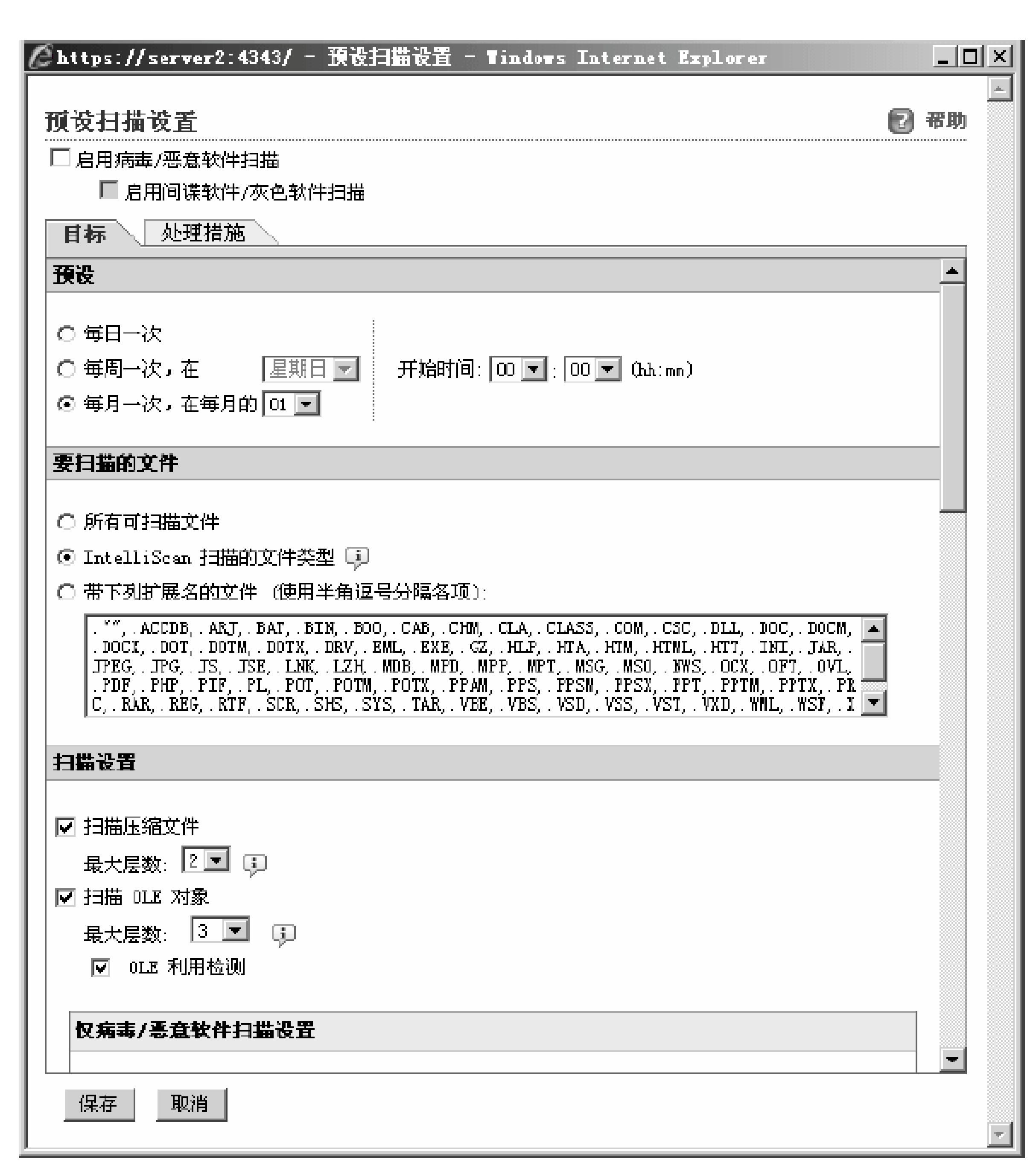


图 15-117

（5）立即扫描设置

如图 15-118 所示，配置完本项设置后，系统会直接应用该项进行扫描。



图 15-118

05 单击【日志】按钮，弹出其下拉列表，可以通过多项设置进行日志管理，选择【病毒/恶意软件日志条件】选项，如图 15-119 所示。



图 15-119

06 弹出【病毒/恶意软件日志条件】页面，如图 15-120 所示，可以设定记录日志的条件，默认记录七天内的所有扫描类型的日志，并按照时间进行排序保存，单击【显示日志】按钮，可以查看已存日志。



图 15-120

07 如图 15-121 所示，单击【管理客户端树】按钮，弹出其下拉列表，有多项配置可以用于管理客户端树。这些项目主要用于层次化的管理客户端。

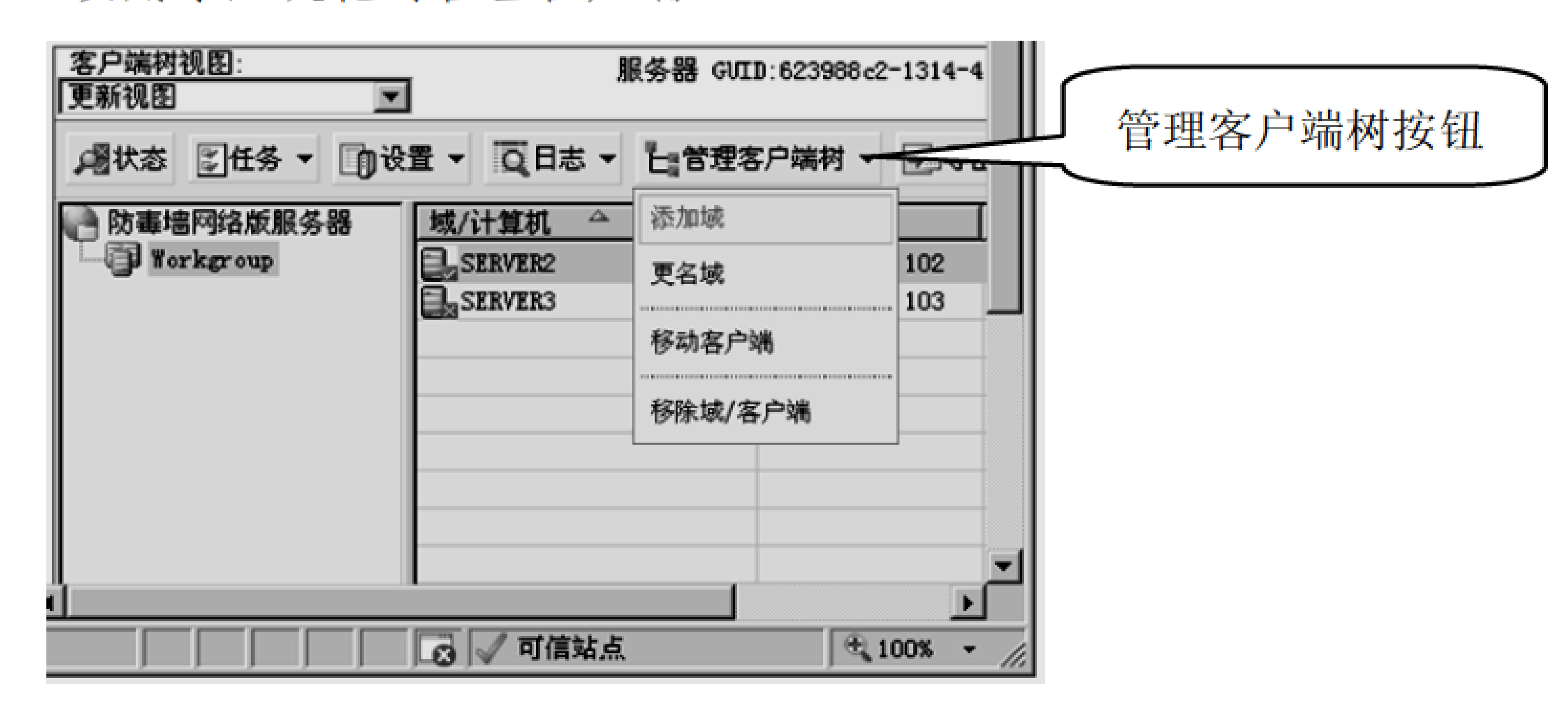


图 15-121

（1）添加域

如图 15-122 所示，在【域名】文本框中可以输入新的区域名，该区域名可以按照部门、职能、地理进行添加，输入完成后单击【添加】按钮。



图 15-122

如图 15-123 所示，新添加了一个区域，名为“Server1”。



图 15-123

（2）移动客户端

添加了新区域后，需要把对应的客户端加入到该域。首先选择指定的客户端，选择【移动客户端】菜单命令，在弹出的【移动客户端】页面选择指定的区域名，如图 15-124 所示，单击【移动】按钮。

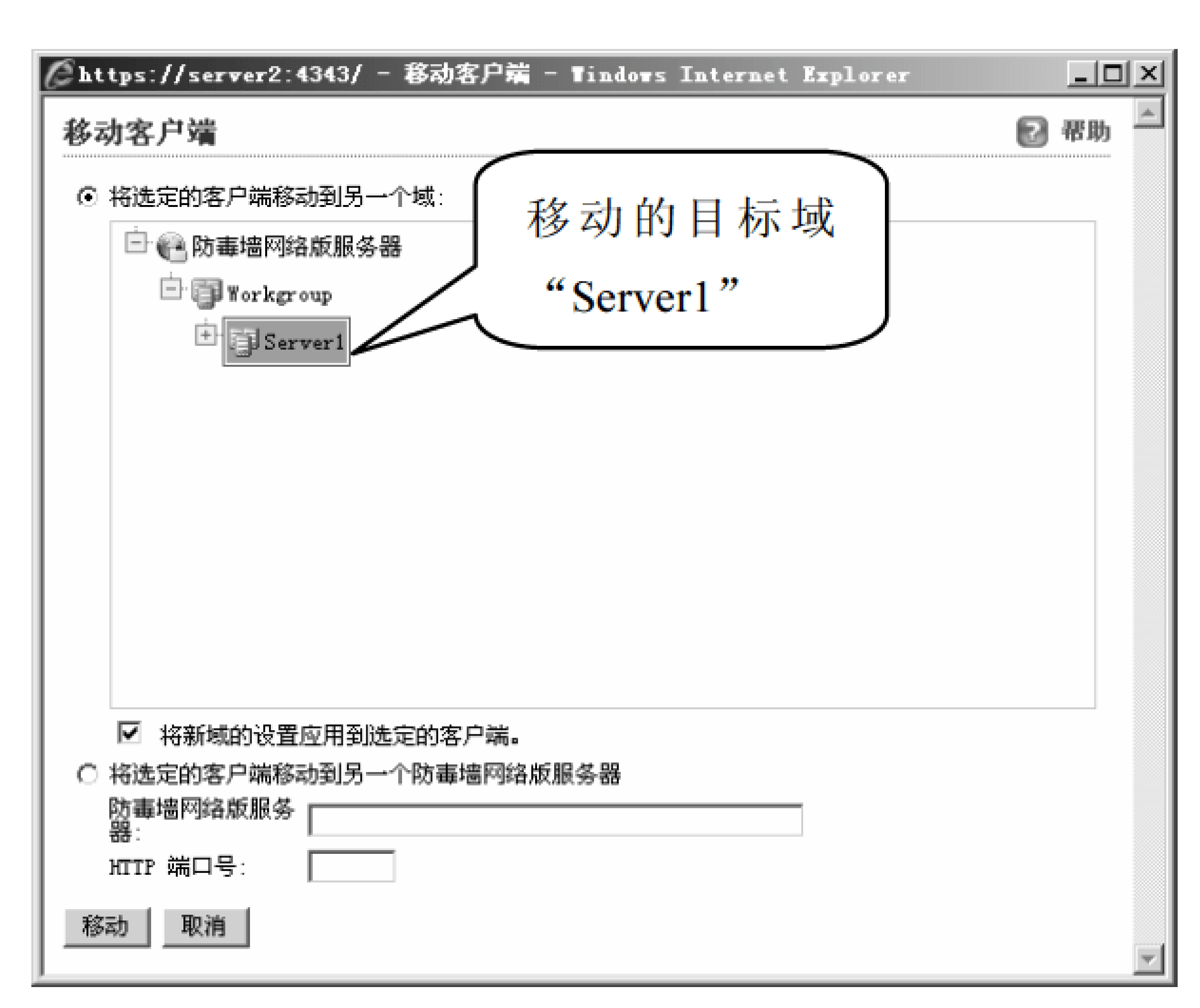


图 15-124

移动成功，已经将一台客户机移动到了“Server1”区域中，如图 15-125 所示。



图 15-125

4. 爆发阻止

当网络中某一主机感染病毒后，如果不及时处理，很可能会散播到全网络，造成巨大的损失。此时，只要将该主机从当前网络中断开，单独查杀病毒即可解决问题。

通过趋势科技网络版防毒墙可以进行网络扫描，及时发现感染病毒的主机，同时可以利用其【爆发阻止】功能将被感染主机网络暂时断开，进行病毒清理。如图 15-126 所示，具体的操作方法为：在左侧列表中选择【联网计算机】➢【爆发阻止】选项，右侧显示【爆发阻止】窗格，在列表中指定需要开启【爆发阻止】功能的计算机，单击【启动爆发阻止】按钮即可。

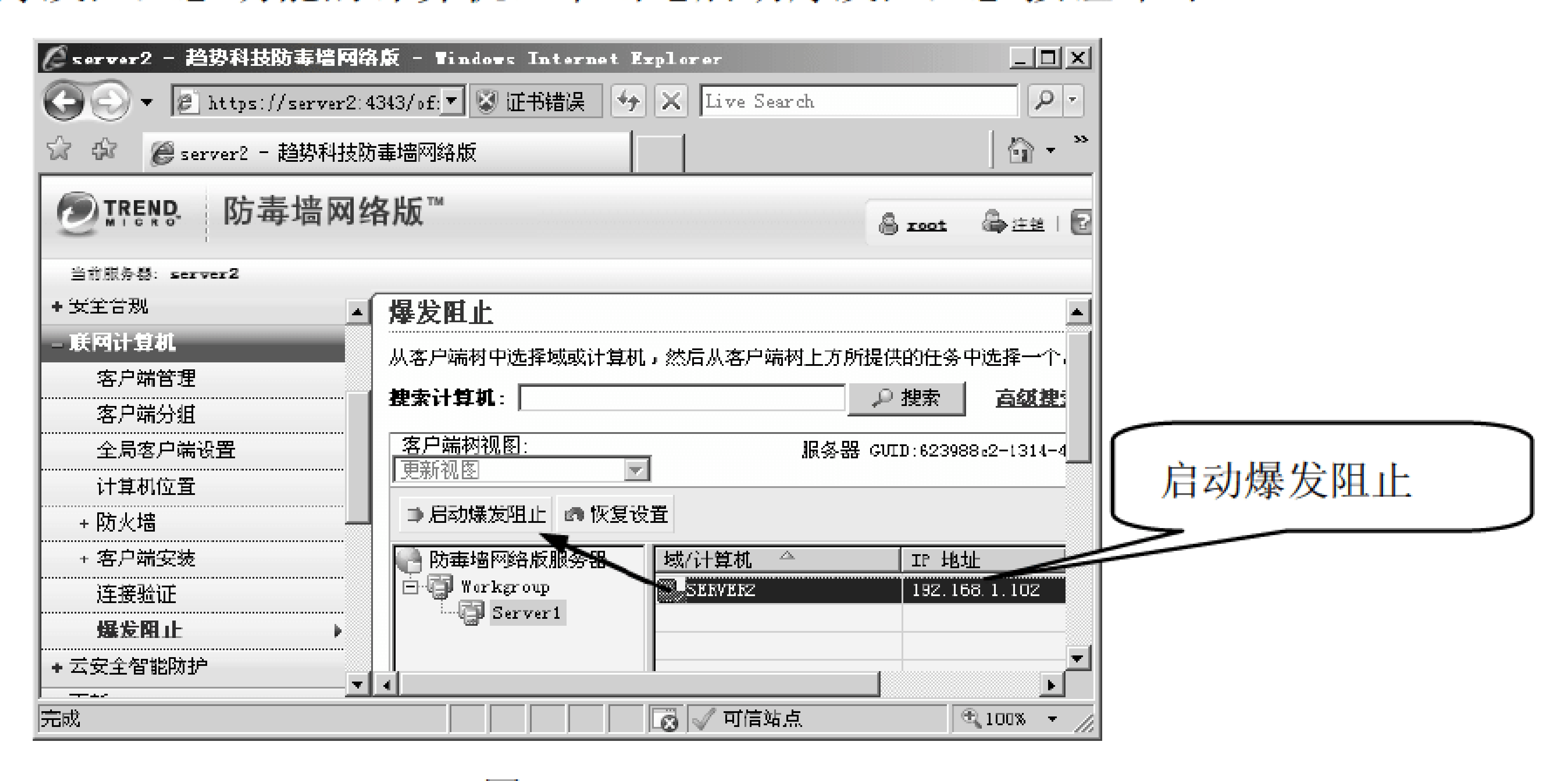


图 15-126

15.3.3 使用趋势科技软件进行全网杀毒

在使用趋势科技进行网络杀毒时，主要有两种方式，分别是：管理员统一全网杀毒和客户机自主杀毒。

1. 全网同步杀毒

当网络中感染病毒后，只是单一的对个别主机进行病毒查杀并不能彻底清除病毒，当病毒突然爆发时，依靠计划任务也不现实，这就需要管理员进行全网同步杀毒操作。具体的操作步骤如下。

01 如图 15-127 所示，选择程序主页面左侧列表中的【立即扫描所有域】选项，弹出【立即扫描】页面，可以实现全网病毒扫描。



图 15-127

02 如图 15-128 所示，在该页面中选择需要扫描的计算机，单击【启动立即扫描】按钮，开始扫描。

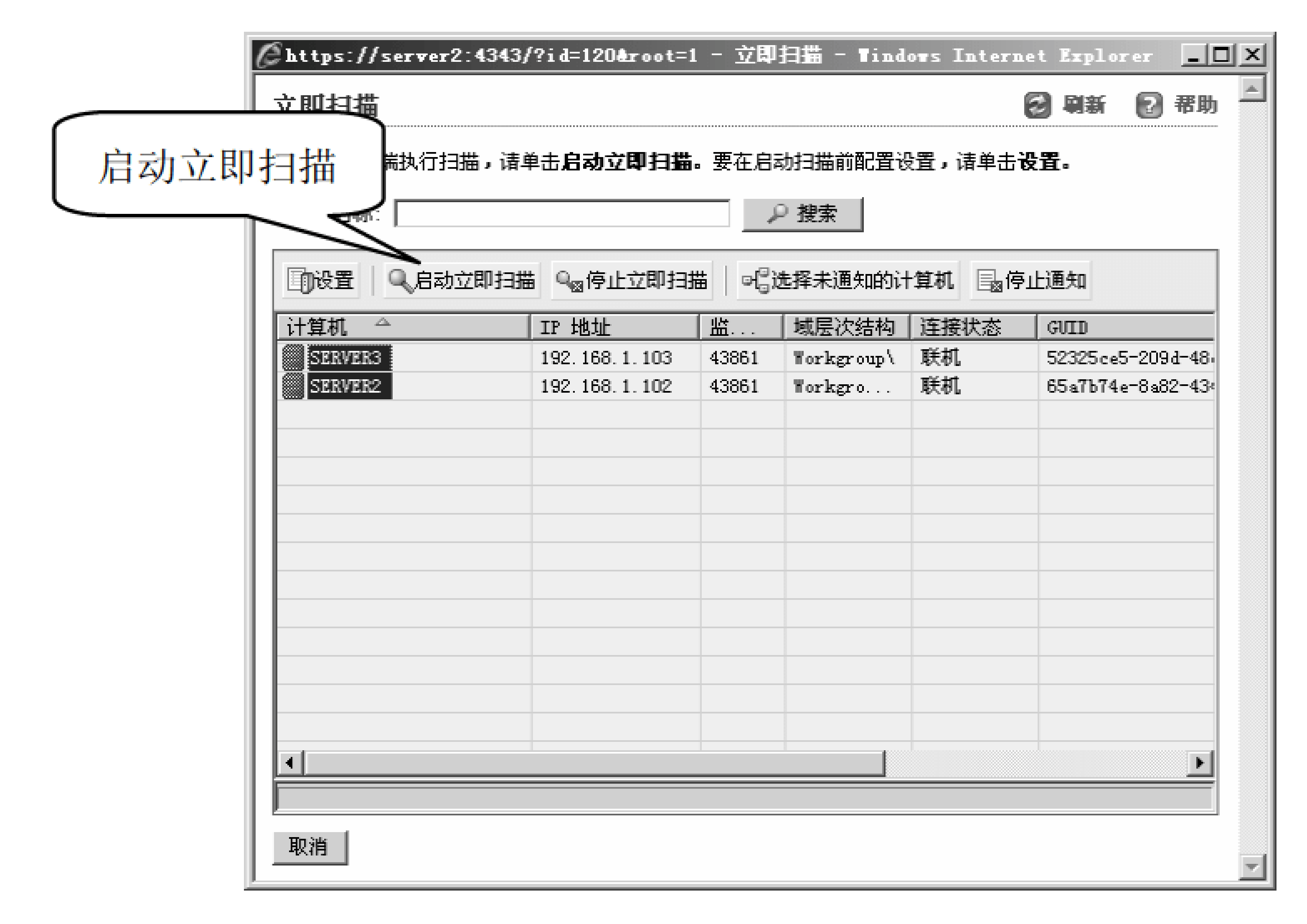


图 15-128

03 扫描结束后，弹出一个信息提示框，如图 15-129 所示，提示用户确认收到通知的客户端只有一个，另一个可以尝试重新连接扫描。

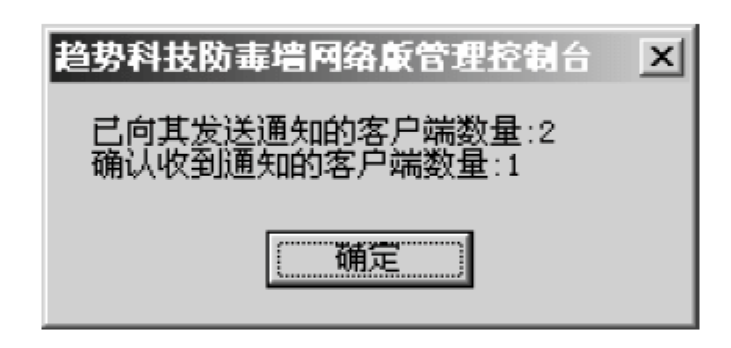


图 15-129



还可以在程序主界面中选择【联网计算机】➢【客户机管理】选项，在右侧窗格中选择所有计算机，单击【任务】下来菜单的【立即扫描】菜单命令实现全网扫描，如图 15-130 所示。



图 15-130

2. 客户端程序杀毒

当客户机感染病毒后，为了及时清理，用户可以手动对自己的主机进行病毒查杀，具体的操作步骤如下。

01 运行趋势科技客户端防毒软件，弹出如图 15-131 所示的对话框，在【手动扫描】选项卡中勾选需要扫描的驱动器符号，单击【扫描】按钮，开始扫描选择驱动磁盘。



图 15-131

02 扫描完成后，在【手动扫描结果】选项卡中显示了扫描结果，如图 15-132 所示。

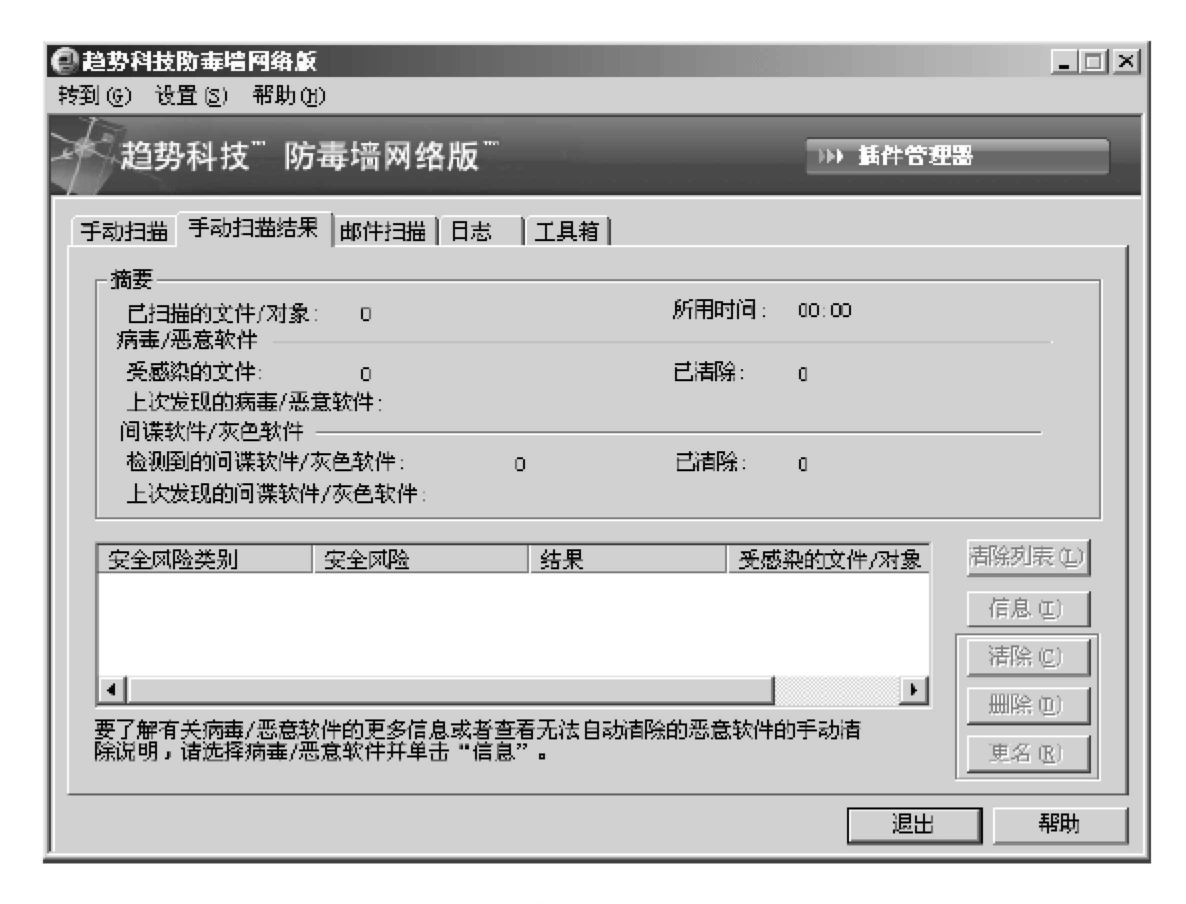


图 15-132

03 选择【邮件扫描】选项卡，在打开的界面中勾选【从邮件服务器下载 POP3 邮件和附件是进行扫描】复选框，开启邮件扫描功能，如图 15-133 所示。

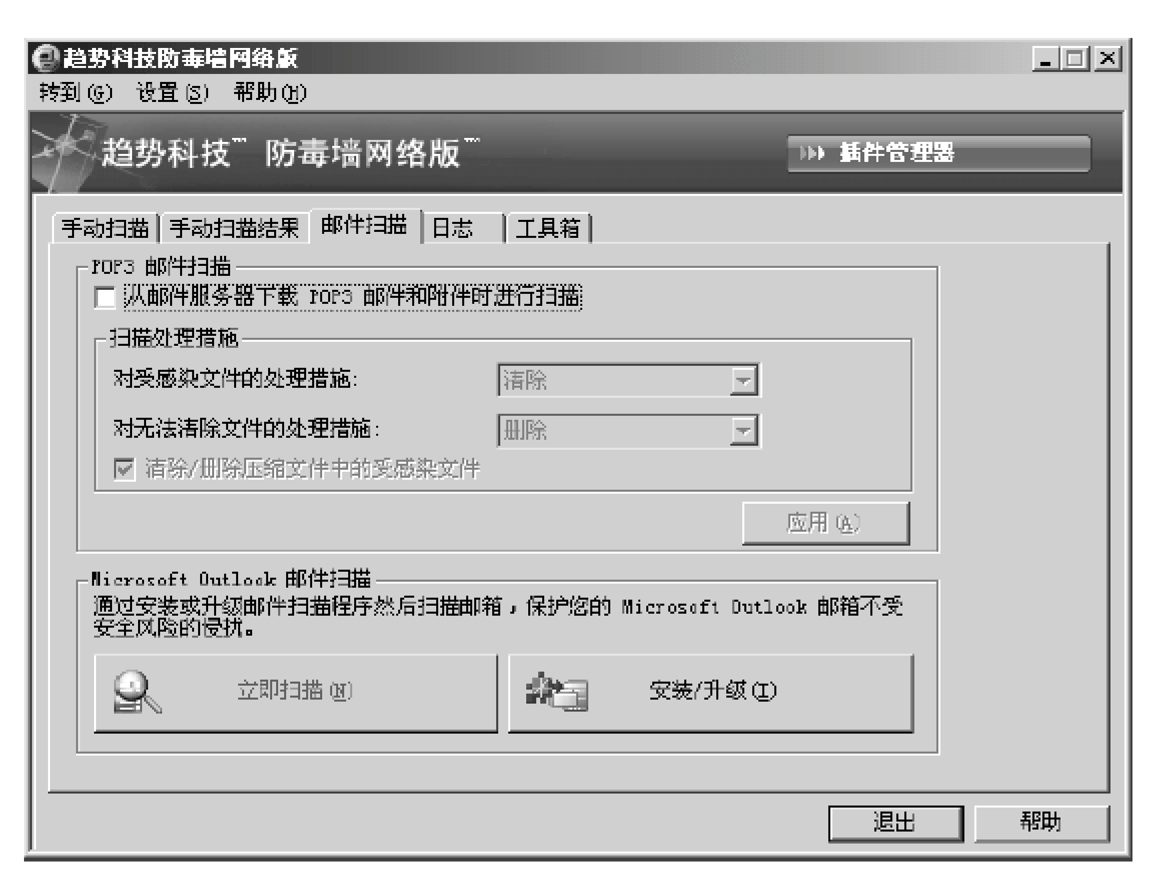


图 15-133

04 选择【日志】选项卡，如图 15-134 所示，在选项卡界面中选择日志类型，并指定日期范围，单击【查看日志】按钮，可以翻阅日志查找故障。



图 15-134



由于日志占用的空间会越来越大，用户可以单击【编辑】按钮进行日志维护。

15.4 专家答疑

（1）企业架设了反病毒系统，为什么还总是有大量病毒传播？

答：架设了反病毒系统后，没有达到病毒防护的原因有以下几点。首先，可能是企业网络感染了新的病毒，而病毒库没有得到及时更新，导致该病毒无法被发现。其次，架设企业反病毒系统时，必须要保证所有主机都处于企业反病毒系统中，如果部分新加主机没有配置反病毒客户端，很可能成为整个网络病毒肆虐的源头，即便是网络管理员一再的查杀，但是始终清除不了这些主机的安全隐患。再次，反病毒系统架设好之后，要配置合理的病毒查杀计划任务，并要定期手动全网查杀病毒，病毒查杀配置可以设置为深度扫描。最后，网络管理员需要规范员工的上网行为和计算机使用行为，从根源上减少计算机病毒流入网络。

（2）反病毒系统程序升级和病毒库更新为什么总是出现失败？

答：首先要强调的是，反病毒程序和病毒库必须要及时更新，如果不能更新，要及时解决问题。出现更新失败的主要原因有以下几点。首先，可能是程序的注册信息过期或错误，需要找客服询问，或到其产品官网更新注册信息。其次，可能是反病毒系统无法连接到更新服务器，可以查看其更新服务器的地址配置是否正确，如果不确定可以指定自动获得服务器地址或者到官网查询更新服务器地址。再次，本地网络连通性也会影响更新，可以使用 PING 命令检测服务器是否连通。最后，也有可能是系统服务冲突，但是一般不会出现冲突现象，如果真是，可能需要进行详细的系统分析。

第 16 章　VPN 虚拟专用网

传统的网络一般局限于一定的区域内，即便一个企业的多个分支机构需要跨越区域互联，也会采用帧中继、专线等广域网技术进行连接。但由于传统方式费用高，架设复杂，很难满足日益增加的网络应用需求，需要有更便捷、更安全，更节约的方式进行跨区域分支连接。VPN 虚拟专用网技术就应运而生了。

16.1　VPN 技术介绍

VPN 技术从产生至今，得到了飞速的发展和社会的认可，各行各业都在使用这项技术，它的出现使得帧中继和专线技术几乎被淘汰。

16.1.1　VPN 技术概述

VPN(Virtual Private Network)，即虚拟专用网络，该技术用于实现局域网络之间通过 Internet 公共网络安全地传递数据。

互联网是目前最大的公共网络，其内有充足的资源可以利用。VPN 技术就是利用这一点，在 Internet 公共网络内部构建一条虚拟的连接广域网中不相邻的两个局域网的链路，该链路可以实现数据安全可靠的传输。

VPN 技术的特征可以总结为以下几点。

（1）在混杂的公用网络（通常是 Internet 网络）中建立一条临时的、安全的连接，是一条横穿公用网络的安全、稳定的隧道。

（2）具有强大的安全加密技术。

（3）可用于满足企业内部网络扩展的需求，允许与远程用户、分支机构和商业伙伴的内部网络商建立安全可靠的连接。

（4）解决了不断增长的移动办公用户互联网访问需求的问题。

16.1.2　VPN 的优点

VPN 技术和传统的网络互联技术比较起来有很多优势，比如解决了长距离通信的费用成本，充分利用了互联网资源，可以实现快速、安全的网络扩展。下面以传统网络中使用比较多的 DDN

专线技术和 VPN 技术作比较。

1. DDN 技术

使用 DDN 专线技术需要在两端局域网之间建立一条与互联网隔离的物理连接链路，DDN 专线技术存在费用高、灵活性差、广域网的管理、拓扑结构复杂等缺点。如图 16-1 所示为其网络拓扑图。

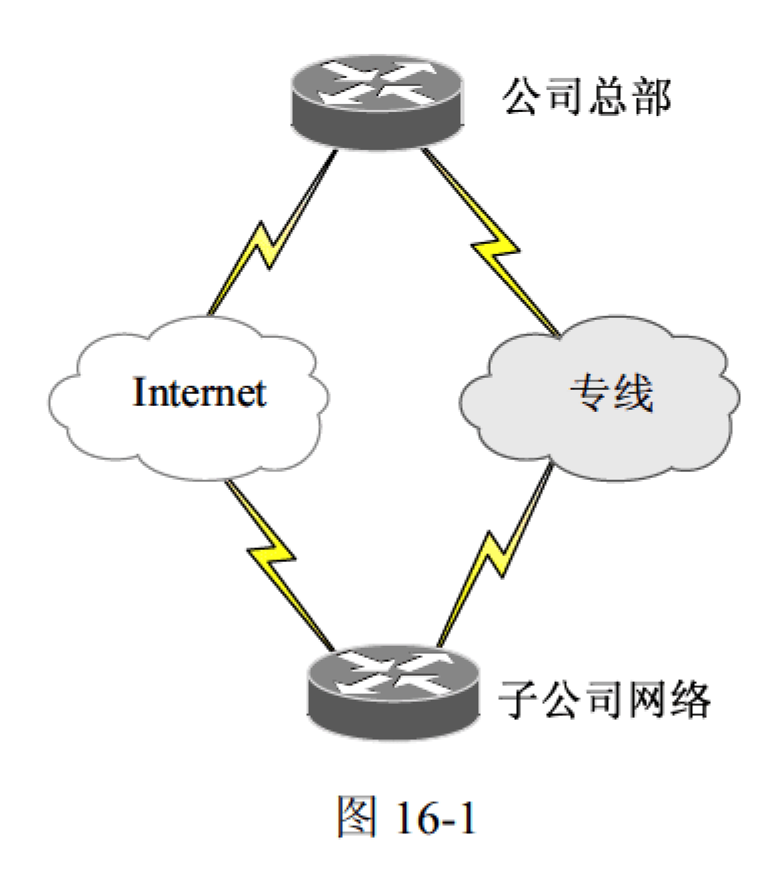


图 16-1

2. VPN 技术

VPN 技术连接时，只要确保两端都可以连接互联网即可实现，如图 16-2 所示为其网络拓扑图。

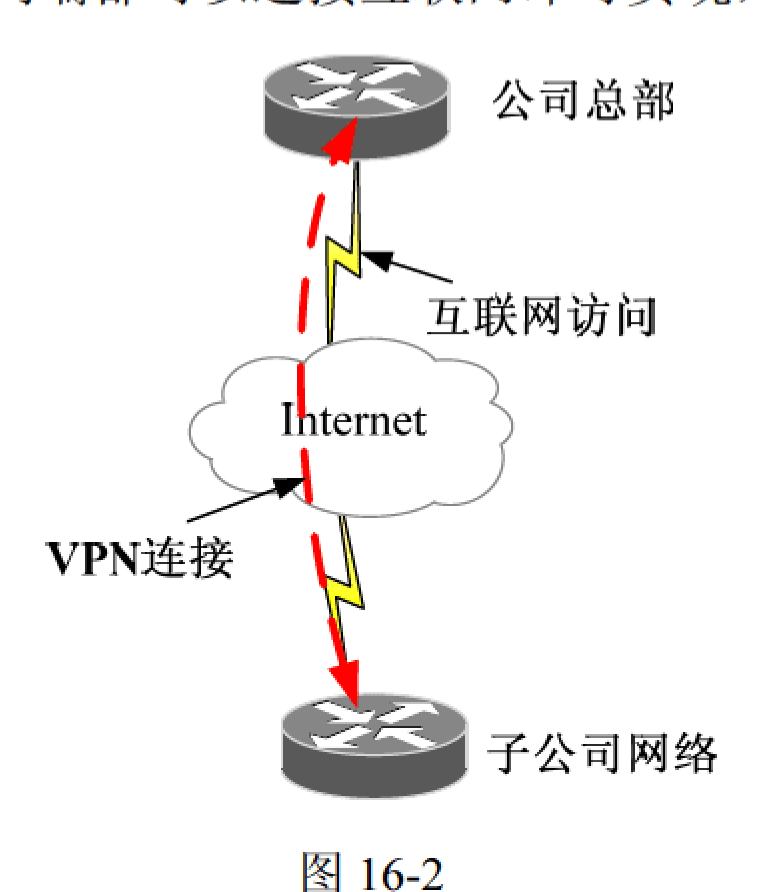


图 16-2

VPN 技术存在费用低、灵活性好、网络管理简单等优点，使用 VPN 技术的优势如下。

（1）节省资金：VPN 技术免去了长途连接的费用，降低了 30%~70%建立私有专网的费用。

（2）用户连接不受地点、网络接入方式的限制，只要用户愿意，可以增加多条连接链路。

（3）提供安全性：具有强大的用户认证机制，可以有效地保障用户数据的安全性、完整性。

（4）配置便捷，不需要对现有网络结构及应用程序做调整。直接在现有环境基础上增加 VPN 配置即可，对于最终用户来说不会感觉到任何变化。

16.1.3 VPN 技术的工作原理

VPN 技术主要依靠认证加密和隧道技术来实现，如图 16-3 所示为其工作原理图。

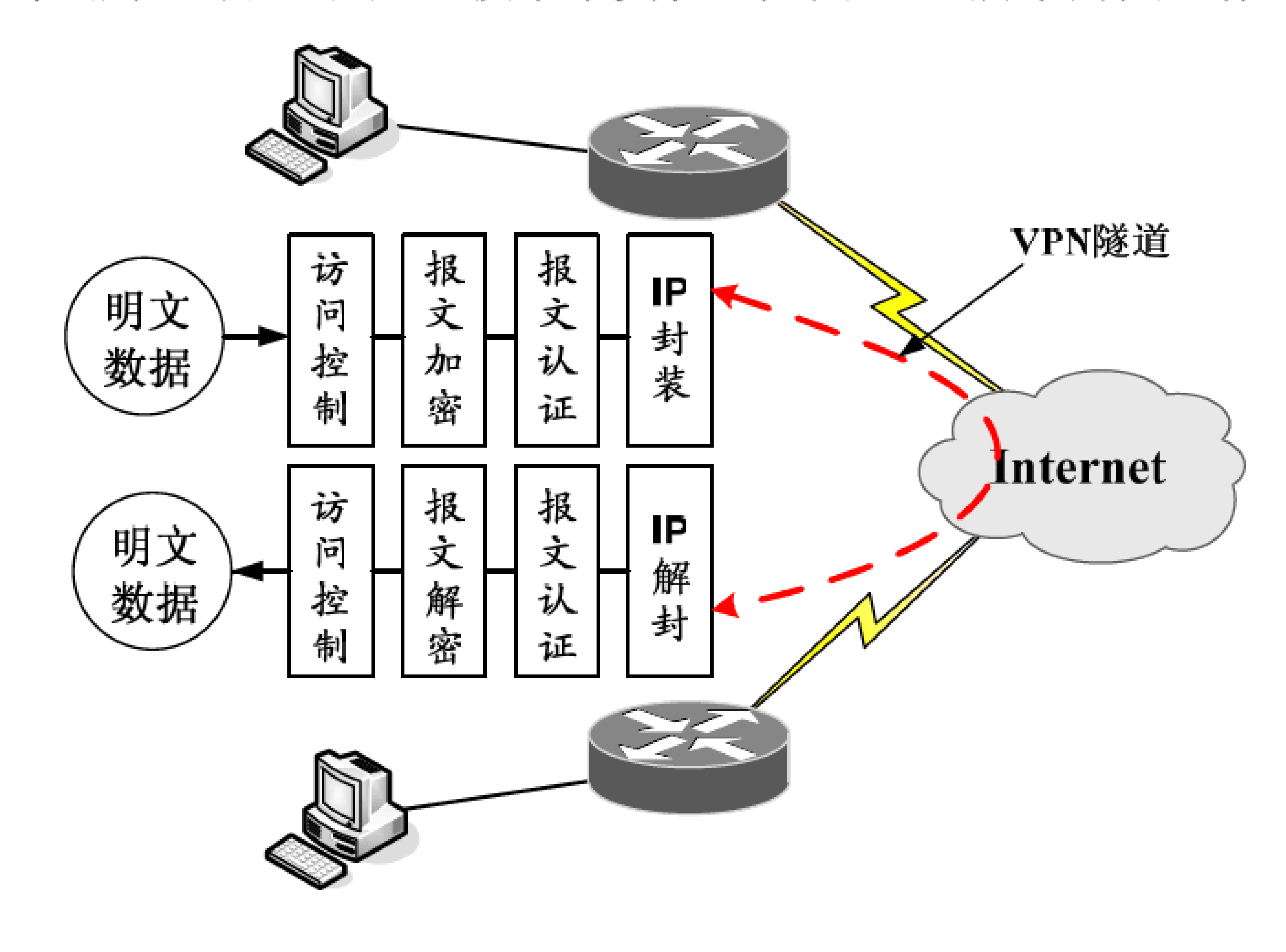


图 16-3

实现 VPN 连接时使用了以下几种技术。

（1）安全隧道技术：隧道是在公共网络上传递私有数据的一种方式，而安全隧道是在公网上几个局域网之间进行数据传输时，保证数据安全及完整的技术。

（2）信息加密技术：用于实现传输过程中数据的安全，VPN 技术采用了多种加密技术，而且可以支持多种加密级别。

（3）用户认证技术：用于确保 VPN 通信方的身份及合法性。

（4）访问控制技术：用于限制 VPN 的通信双方的信息流。

VPN 技术在建立隧道时可以构建二层隧道和三层隧道，分别涉及以下协议。

（1）二层隧道 VPN

- L2TP（Layer 2 Tunnel Protocol）：二层隧道协议，用于实现二层隧道的建立。
- PPTP（Point To Point Tunnel Protocol）：点到点隧道协议。
- L2F（Layer 2 Forwarding）：用于实现二层隧道数据转发。

（2）三层隧道 VPN

- GRE（General Routing Encapsulation）：用于实现三层隧道的建立。
- IPSec（IP Security Protocol）：IP 安全协议，用于实现三层隧道转发时数据的安全加密、认证。

16.1.4 VPN 技术分类

VPN 技术根据两端的连接主体不同，可以分为两种连接方式：远程访问的 VPN 和站点到站点的 VPN。

远程访问的 VPN 适用于建立临时性的 VPN 连接，家庭和移动办公用户使用的比较多。只需

要企业网络中配置有软件或硬件形式的 VPN 设备，移动或家庭办公用户就可以通过自己的客户端操作系统直接建立 VPN 连接请求。

站点到站点的 VPN 连接可以建立长期的 VPN 连接，适合公司总部和子公司之间长期进行数据传输。需要两端网络中都有配置好的 VPN 软件程序或硬件设备，并且有匹配的认证加密配置。如图 16-4 所示为两种连接方式的网络拓补图。

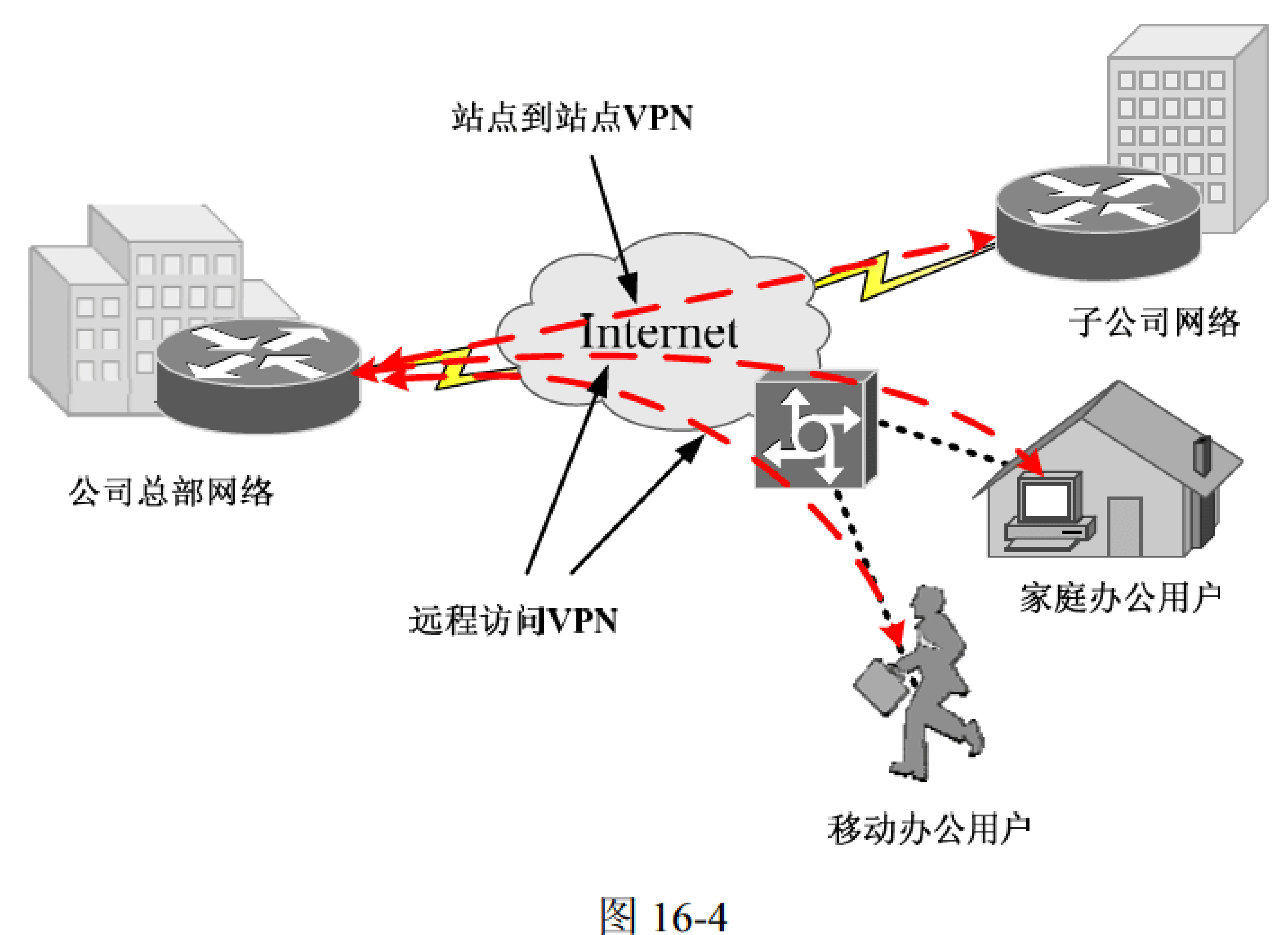


图 16-4

16.2 基于 Windows 的远程访问 VPN

基于 Windows 的远程访问 VPN 的技术一般适用于在外出差或家庭办公的用户访问企业内部网络，如图 16-5 所示为其网络拓扑结构图。

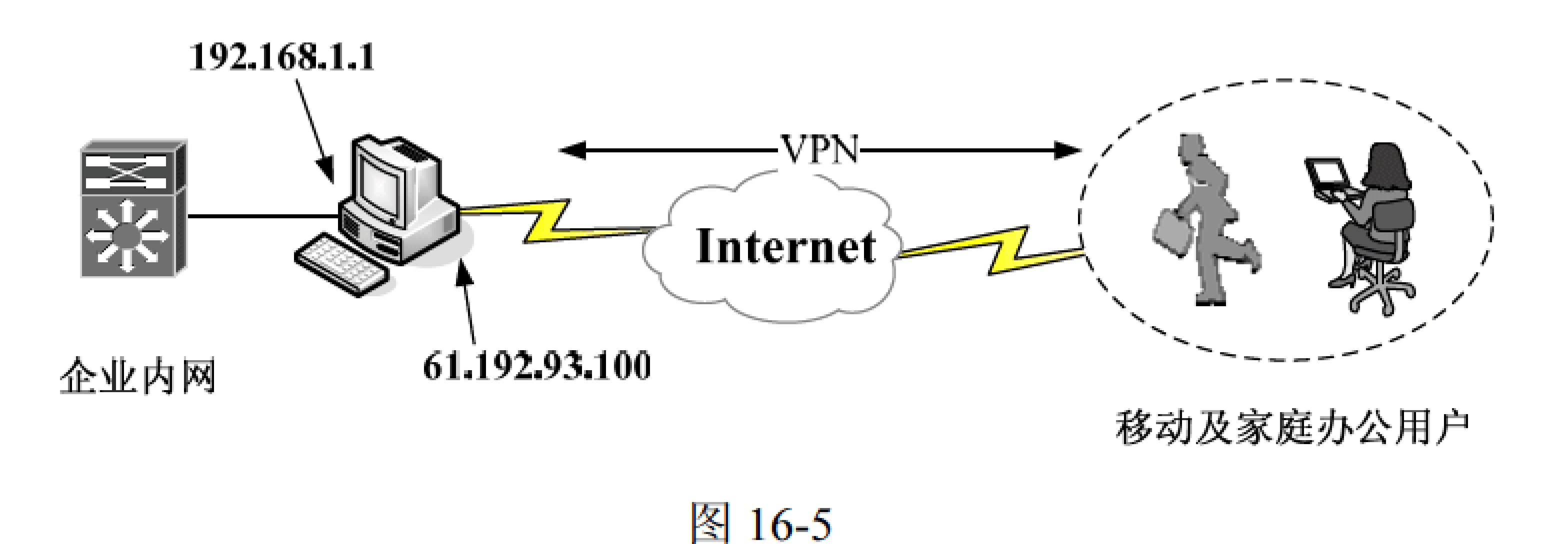


图 16-5

16.2.1 配置远程访问功能

基于 Windows 的远程访问 VPN 功能主要是通过配置“路由和远程访问”管理工具实现的，下面介绍详细配置方法。

1. 开启远程访问功能

首先需要在企业网络出口的服务器上开启“路由和远程访问”功能，具体的操作步骤如下。

01 在桌面选择【开始】➢【程序】➢【管理工具】➢【路由和远程访问】菜单命令，如图 16-6 所示。



图 16-6

02 弹出【路由和远程访问】窗口，默认路由和远程访问功能不开启，图标显示有红色向上箭头，右击路由和远程访问本地服务器图标，在弹出的快捷菜单中选择【配置并启用路由和远程访问】菜单命令，如图 16-7 所示。

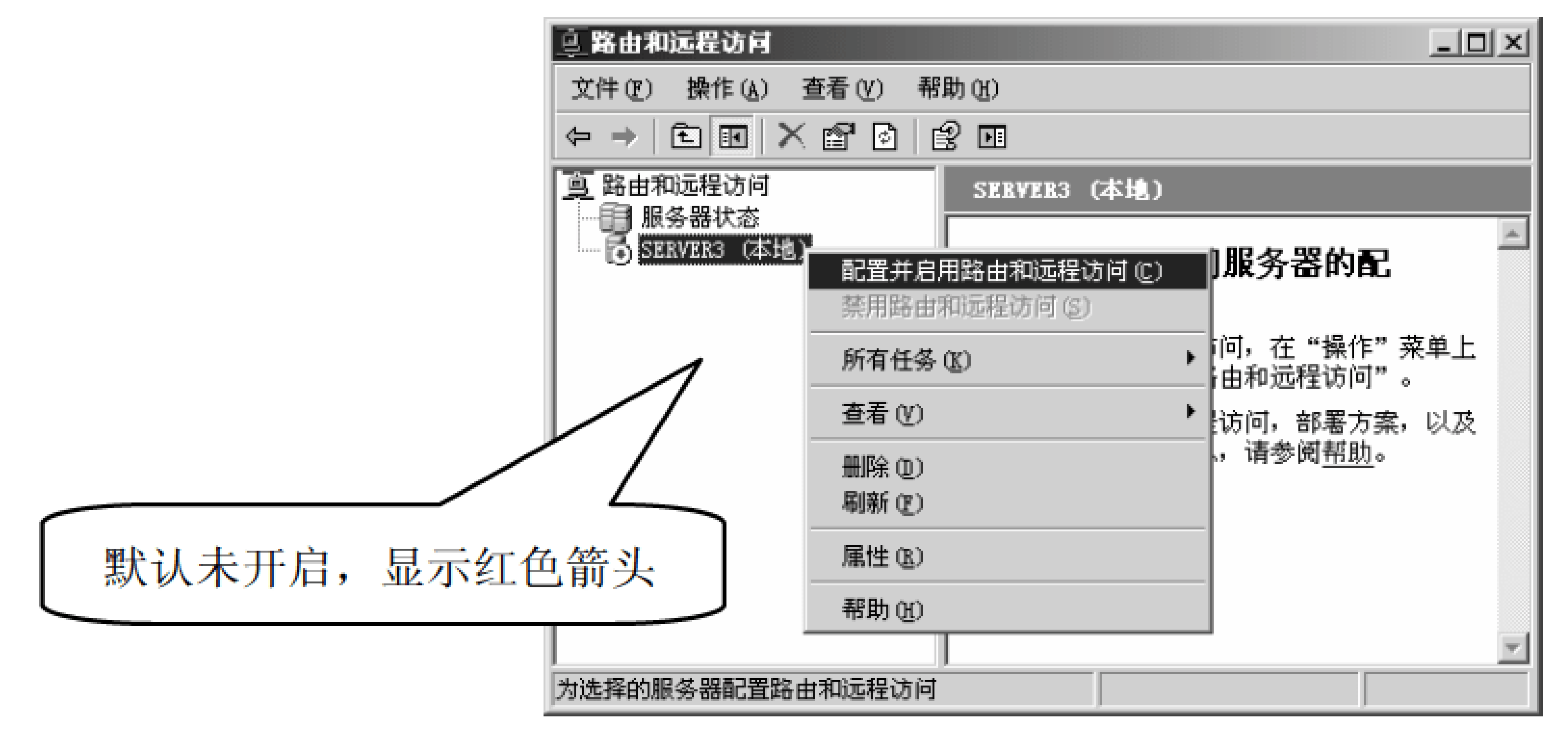


图 16-7

03 弹出开启服务向导对话框，如图 16-8 所示，单击【下一步】按钮。



图 16-8

04 弹出【配置】对话框，由于本机属于出口设备需要同时具有路由的 NAT 功能和 VPN 功能，所以选择【虚拟专用网（VPN）访问和 NAT】单选按钮，单击【下一步】按钮，如图 16-9 所示。

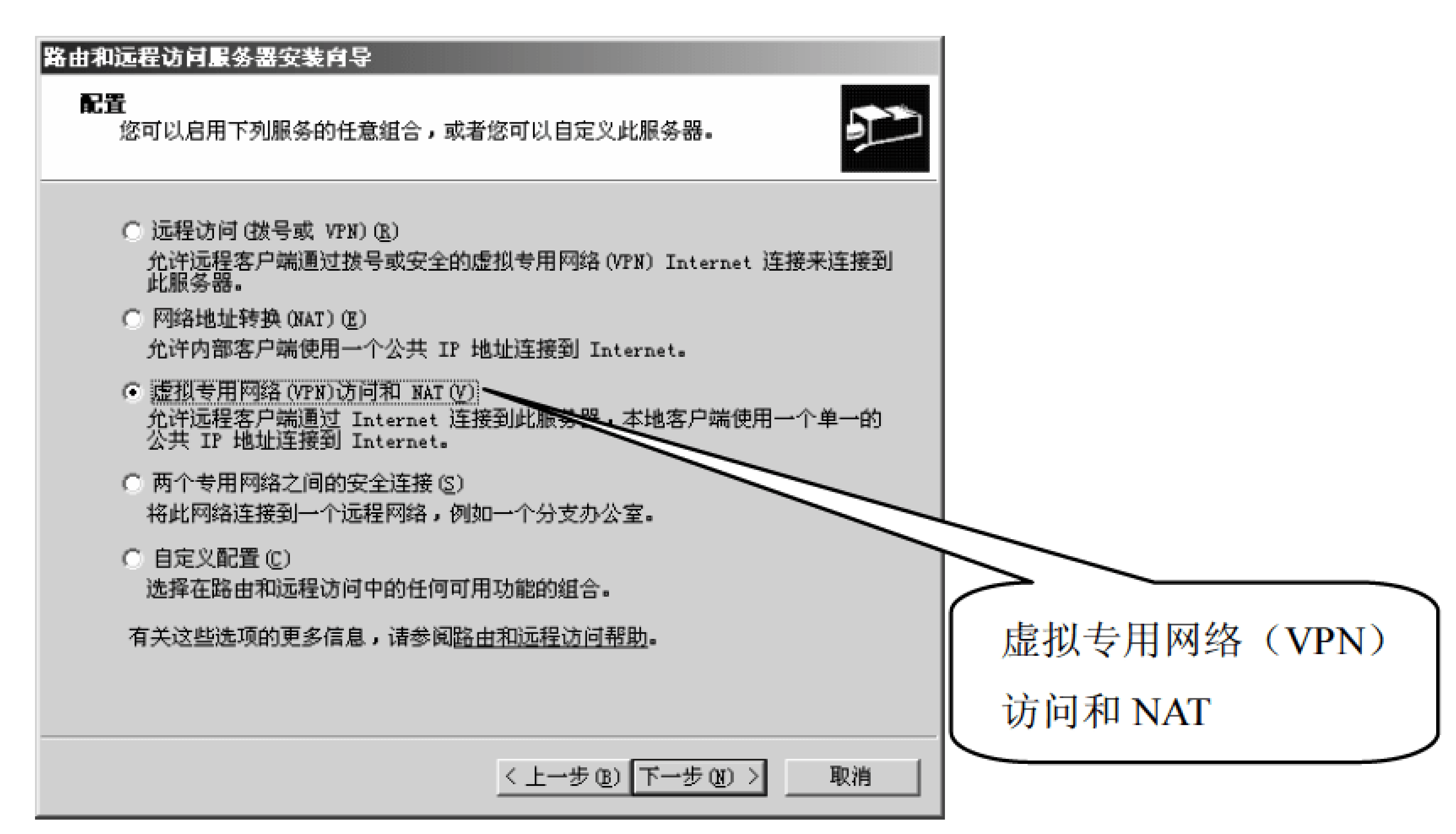


图 16-9

05 弹出【VPN 连接】对话框，在网络接口窗格中显示了本地的两个网卡信息，选择外网网卡，如图 16-10 所示，单击【下一步】按钮。

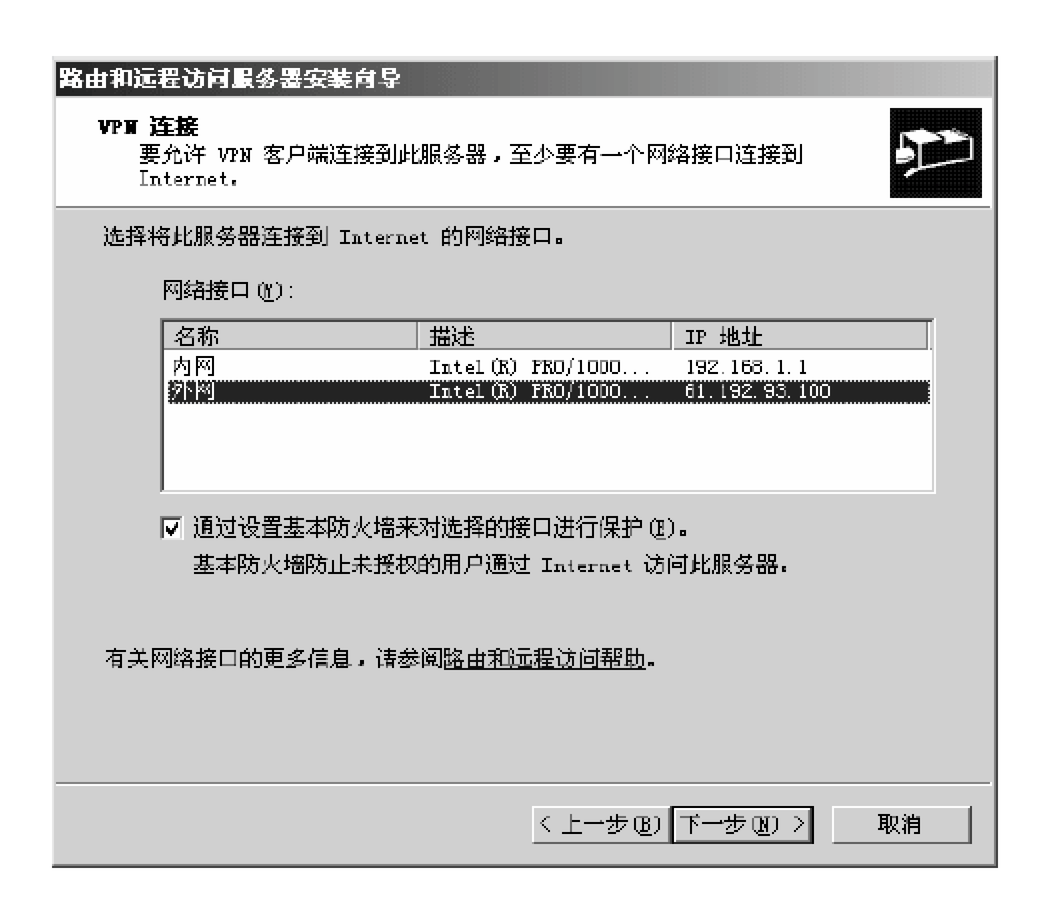


图 16-10

06 弹出【IP 地址指定】对话框，选择【来自一个指定的地址范围】单选按钮，如图 16-11 所示，使远程移动 VPN 客户端主机使用指定的 IP 地址访问内网，单击【下一步】按钮。

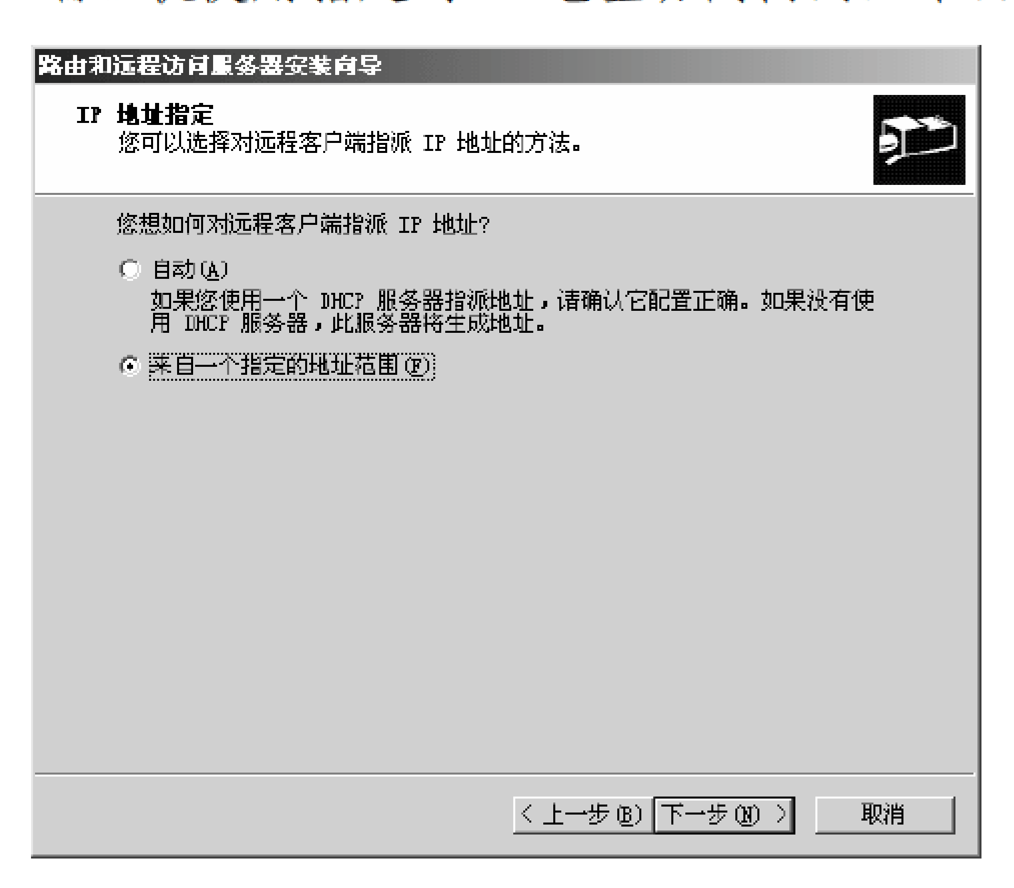


图 16-11

07 弹出【地址范围指定】对话框，如图 16-12 所示，单击【新建】按钮，创建远程 VPN 客户机可以使用的地址段。

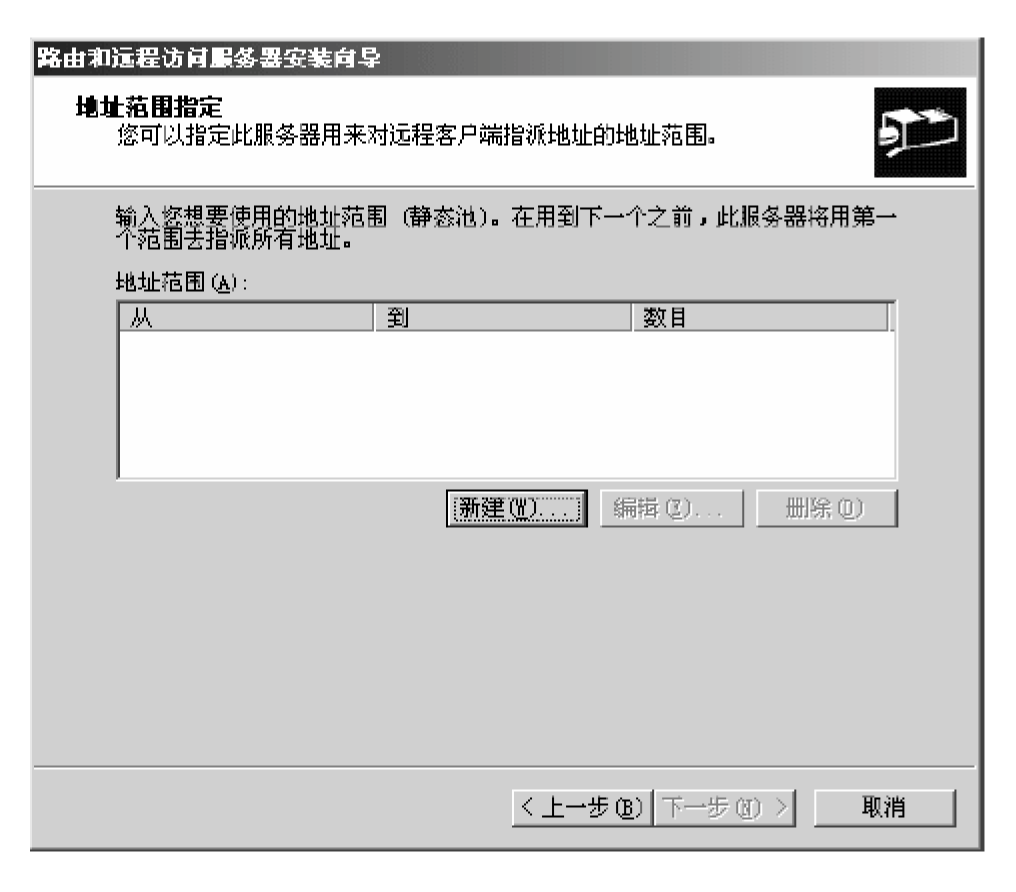


图 16-12

08 弹出【新建地址范围】对话框，在【起始 IP 地址】和【结束 IP 地址】文本框中配置地址范围，本实例采用“192.168.1.100~192.168.1.200”地址段，在【地址数】文本框显示了可用地址数量，如图 16-13 所示，单击【确定】按钮。

新建地址范围
输入一个起始 IP 地址，和结束 IP 地址或范围中的地址数。
起始 IP 地址(S): 192.168.1.100
结束 IP 地址(E): 192.168.1.200
地址数(N): 101
确定　取消

图 16-13

09 返回【地址范围指定】对话框，在【地址范围】列表中显示了新建的地址段，如图 16-14 所示，单击【下一步】按钮。

路由和远程访问服务器安装向导
地址范围指定
您可以指定此服务器用来对远程客户端指派地址的地址范围。
输入您想要使用的地址范围（静态池）。在用到下一个之前，此服务器将用第一个范围去指派所有地址。
地址范围(A):

从	到	数目
192.168.1.100	192.168.1.200	101

新建(W)...　编辑(E)...　删除(D)
< 上一步(B)　下一步(N) >　取消

图 16-14

10 弹出【管理多个远程访问服务器】对话框，可以配置远程客户端身份认证的方式，由于本地没有配置 RADIUS 服务器，选择【否，使用路由和远程访问来对连接请求进行身份验证】单选按钮，如图 16-15 所示，单击【下一步】按钮。

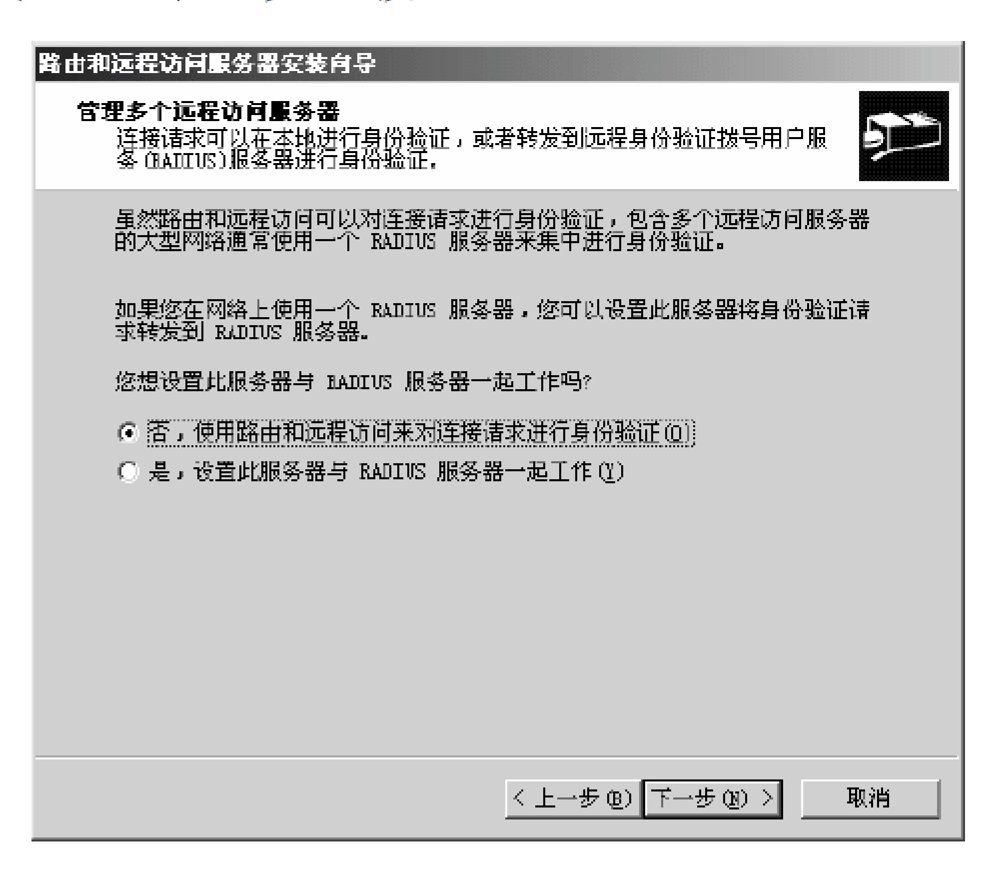


图 16-15

11 配置完成，显示配置的摘要信息，如图 16-16 所示，单击【完成】按钮。

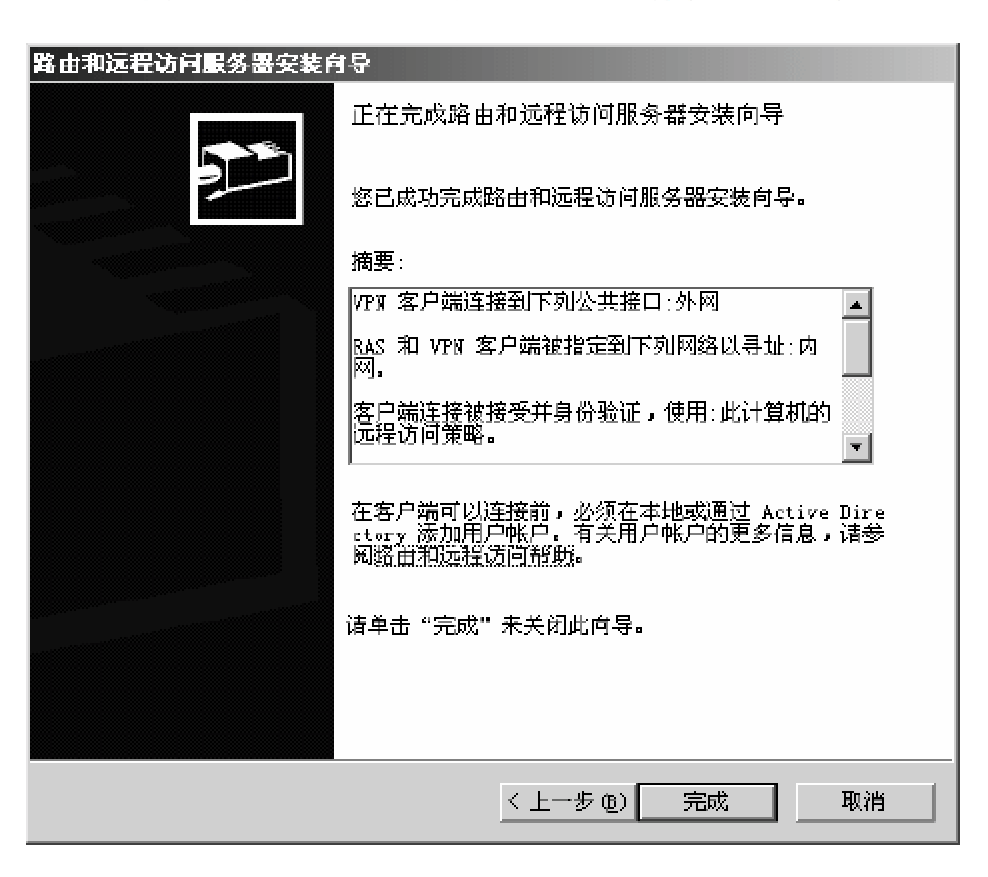


图 16-16

12 弹出 DHCP 消息中继提示框，如果允许远程 VPN 客户端通过企业内网的 DHCP 获得地址，路由和远程访问配置时必须做 DHCP 中继配置，单击【确定】按钮，如图 16-17 所示。

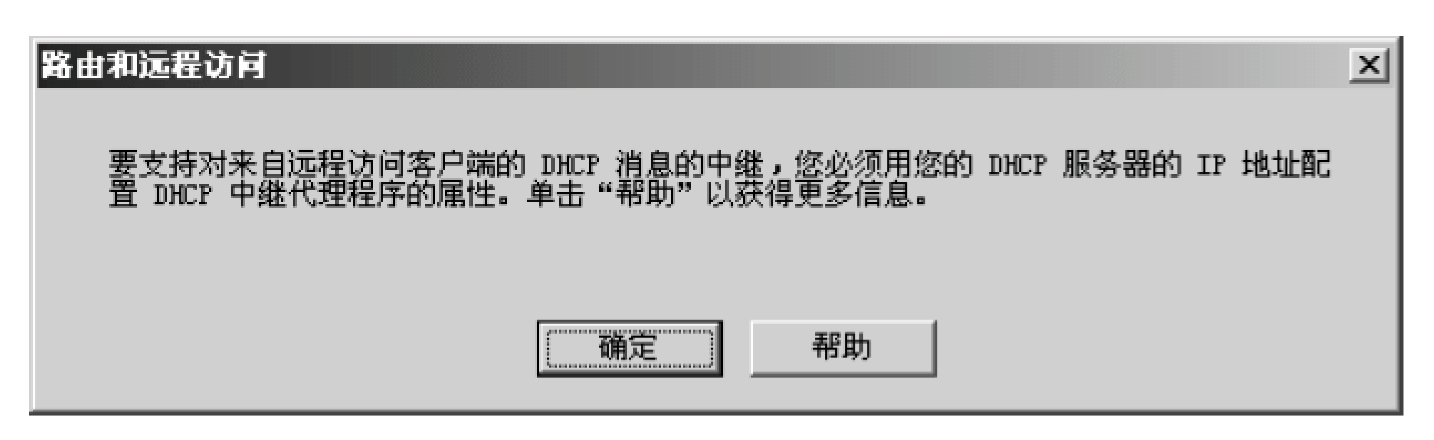


图 16-17

13 路由和远程访问服务开启，该服务包括多种配置信息，如图 16-18 所示。

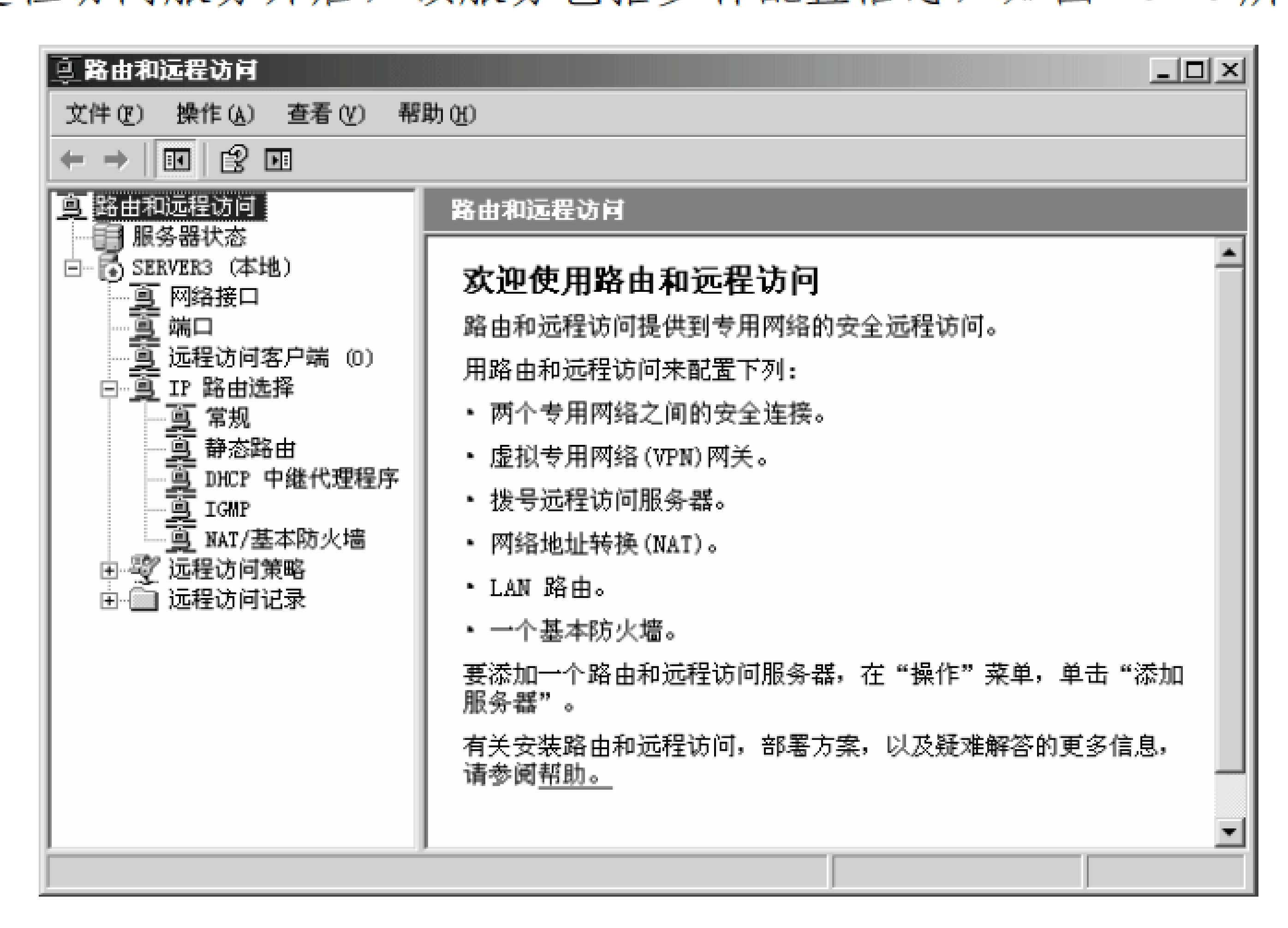


图 16-18

2. 认识路由和远程访问

开启路由和远程访问后，为了方便以后维护管理，还需要对其相关参数进行配置。

（1）网络接口

该选项显示了当前主机的网络接口数量及其功能，不需要做配置。

（2）端口

用于配置客户端可以使用的连接端口类型及数量，具体的配置操作步骤如下。

01 在左侧选项列表中右击【端口】选项，在弹出的快捷菜单中选择【属性】菜单命令，如图 16-19 所示。

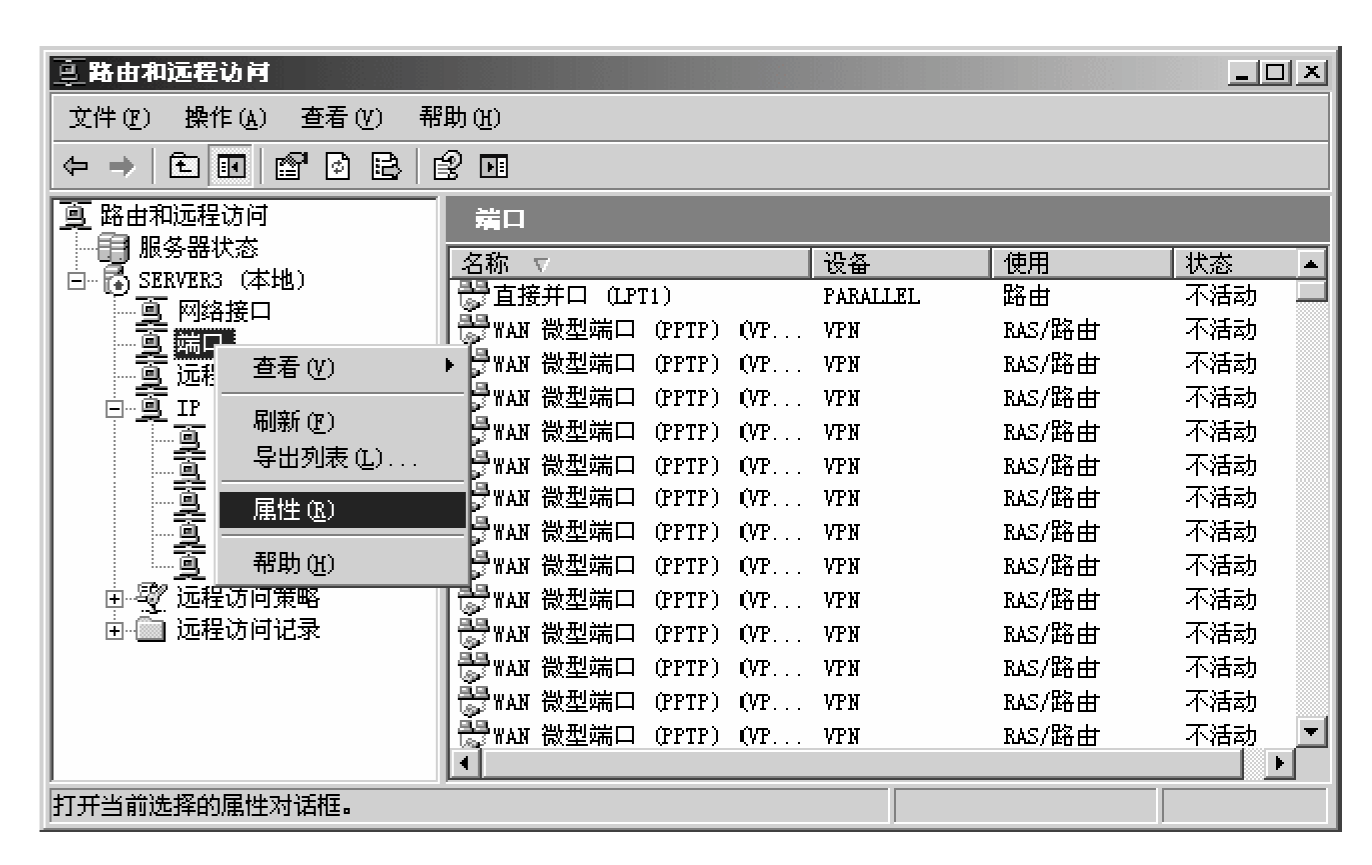


图 16-19

02 弹出【端口 属性】对话框，显示了可以使用的连接端口类型，有 PPPoE、PPTP、L2TP 和并行四种，PPPoE 为用户拨号连接，一般配置 PPTP 和 L2TP 即可，选择 PPTP 选项，单击【配置】按钮，如图 16-20 所示。

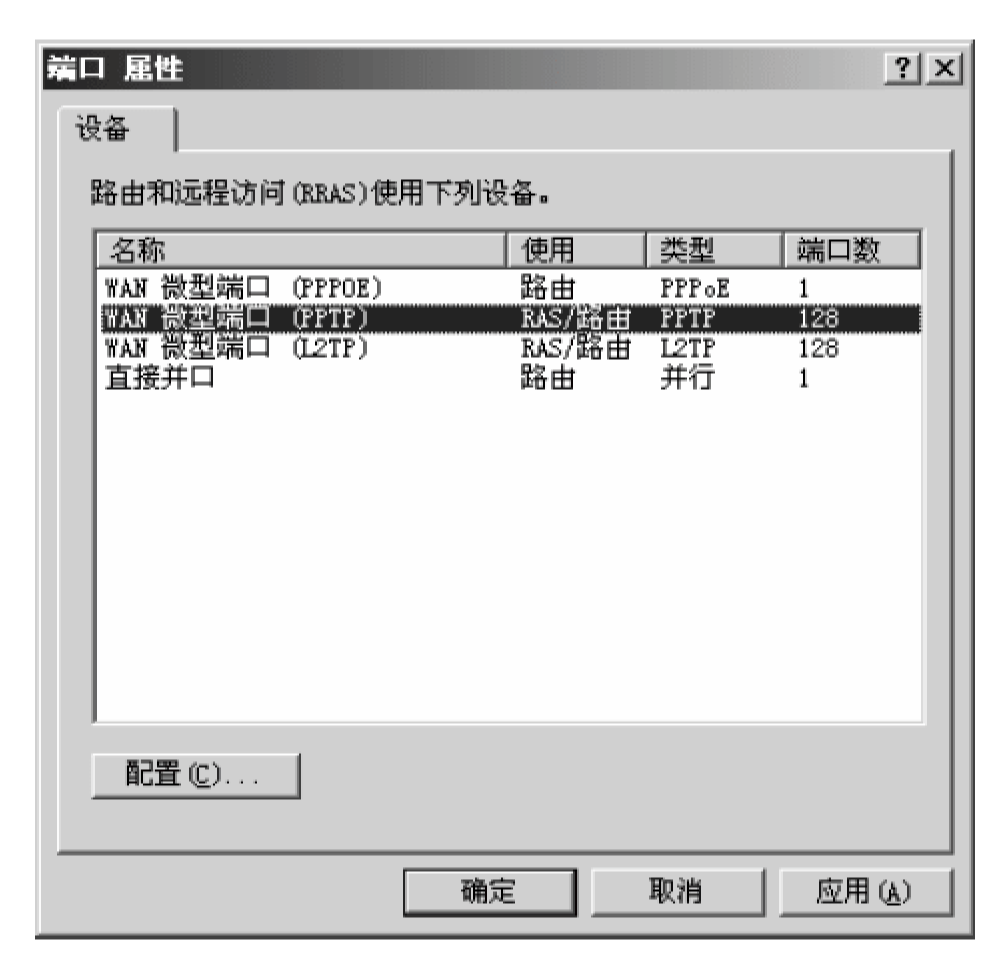


图 16-20

03 弹出【配置设备-WAN 微型端口（PPTP）】对话框，默认配置允许远程访问连接，【最多端口数】文本框可以配置允许使用 PPTP 端口连接的客户端数量，默认为 128 个，全部使用默认配置，单击【确定】按钮，如图 16-21 所示。

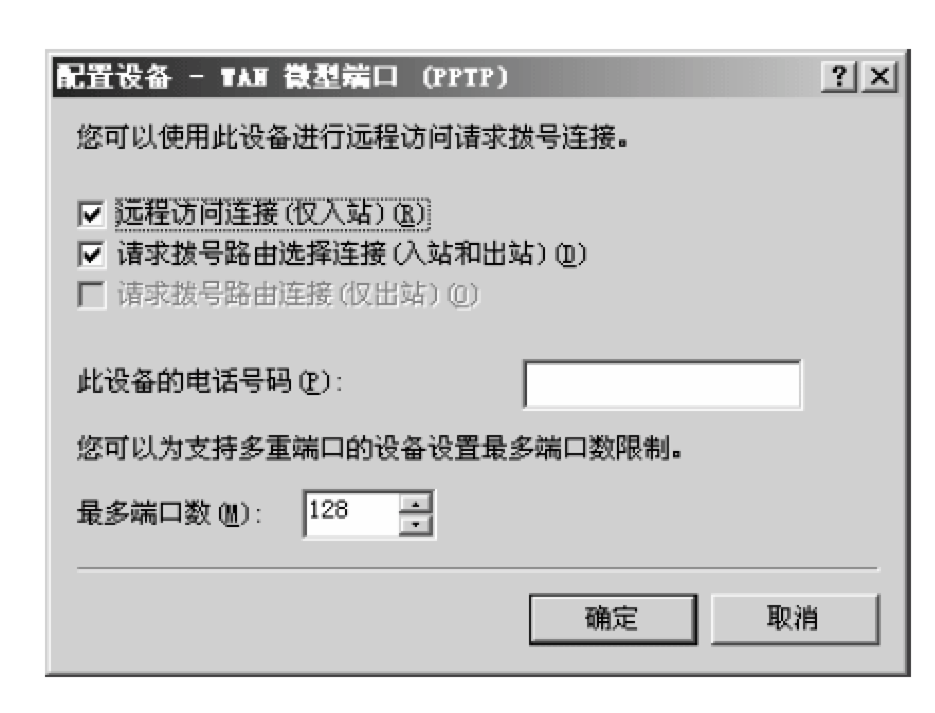


图 16-21

（3）远程访问客户端

选择左侧列表中的【远程访问客户端】选项，可以在右侧查看正在连接的远程访问客户端信息，如图 16-22 所示。



图 16-22

（4）IP 路由选择

如图 16-23 所示，通过该项可以配置本机的路由功能，包括四项信息和配置项，其含义如下。

- 【常规】：用于显示当前网卡信息。
- 【静态路由】：用于配置静态路由条目。
- 【DHCP 中继代理程序】：用于配置其至此的中继代理配置信息。
- 【NAT/基本防火墙】：用于实现内外网地址转换和防火墙策略配置。



图 16-23

16.2.2　远程客户端连接策略配置

客户端在进行连接时需要身份认证，身份认证的配置有两方面内容限制，分别是：允许远程连接的账号本身的拨入配置和远程访问策略的配置。如果远程访问策略做了禁止连接的策略，则停止连接；如果远程策略允许连接，则看用户配置是否允许访问，默认访问策略不做限制。

1. 启用本地用户访问权限

具体的操作步骤如下。

01 在桌面右击【我的电脑】图标，在弹出的快捷菜单中选择【管理】菜单命令，如图 16-24 所示。



图 16-24

02 弹出【计算机管理】窗口，在左侧窗格中选择【计算机管理】➢【系统工具】➢【本地用户和组】➢【用户】选项，本实例使用“user1”账户进行 VPN 连接，右击 user1 账户，在弹出的快捷菜单中选择【属性】菜单命令，如图 16-25 所示。



图 16-25

03 弹出【user1 属性】对话框，选择【拨入】选项卡，在【远程访问权限】中有三个选项，如果不使用远程访问策略，选择【允许访问】单选按钮，单击【确定】按钮即可，如图 16-26 所示。

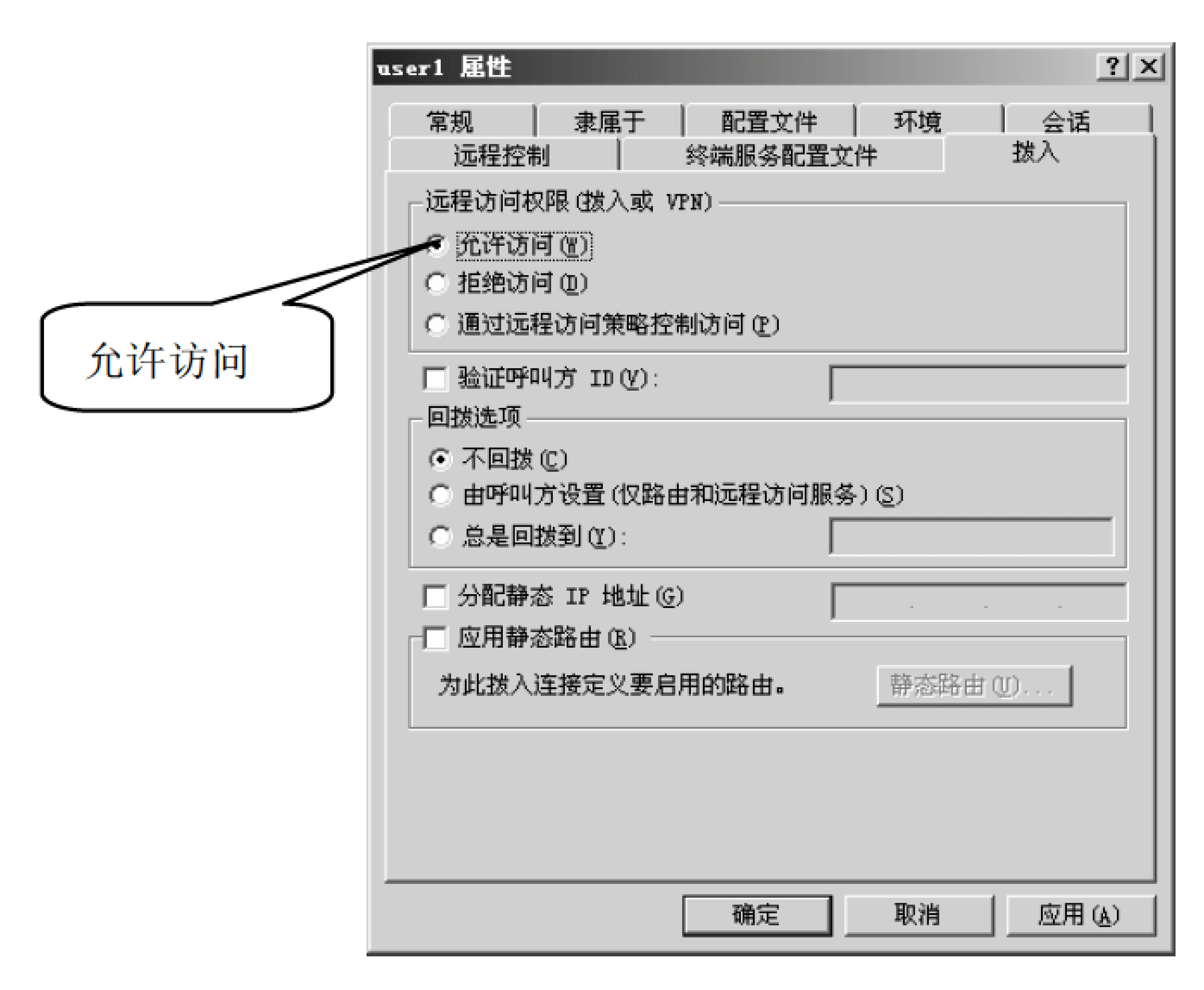


图 16-26

2. 配置远程访问策略

如果在用户属性的【拨入】选项卡中选择【通过远程访问策略控制访问】单选按钮，则需要配置远程访问策略，具体的操作步骤如下。

01 如图 16-27 所示，在【路由和远程访问】窗口左侧选项中选择【SERVER3(本地)】➢【远程访问策略】选项，在右侧窗格中显示了已有的远程访问策略，右击空白区域，在弹出的快捷菜单中选择【新建远程访问策略】菜单命令。

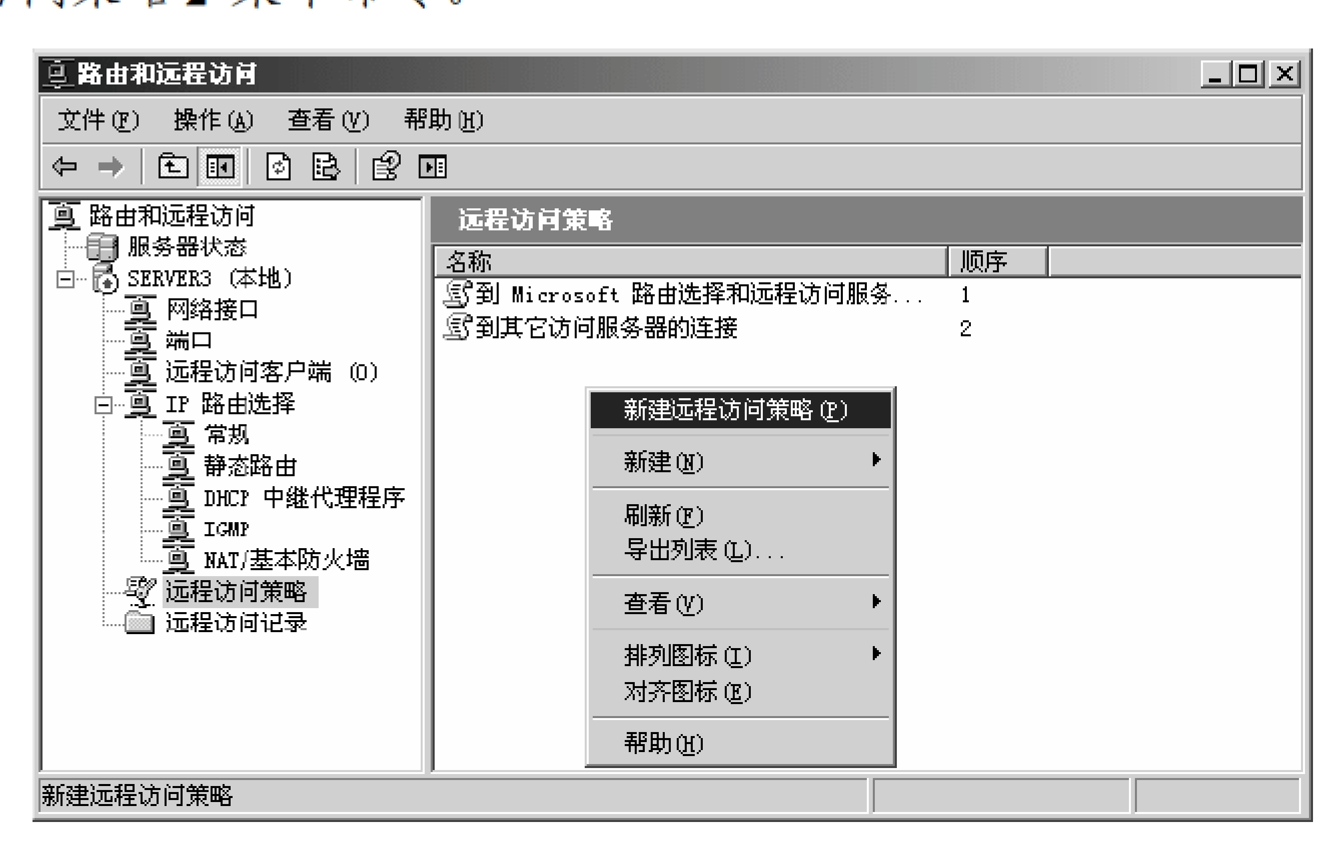


图 16-27

02 弹出【新建远程访问策略向导】对话框，单击【下一步】按钮，如图 16-28 所示。

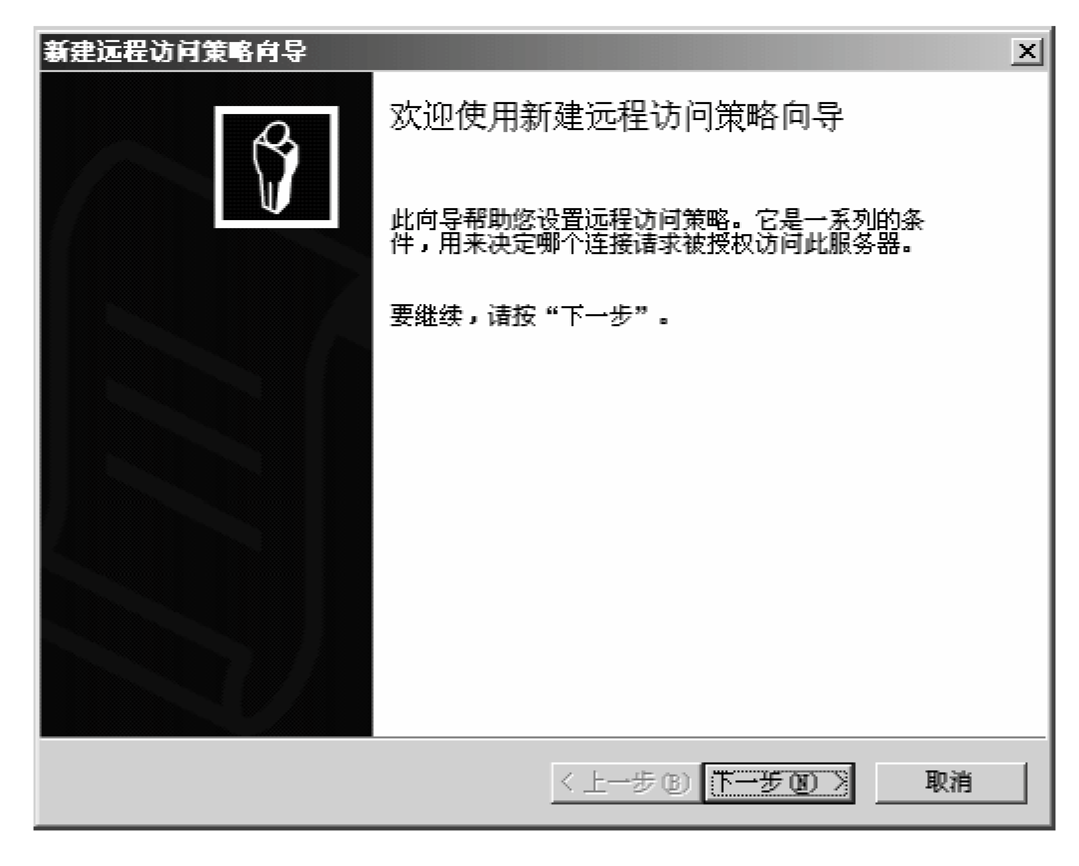


图 16-28

03 弹出【策略配置方法】对话框，选择【使用向导来设置普通情况下的典型的策略】单选按钮，在【策略名】文本框中输入策略名“策略 1”，如图 16-29 所示，单击【下一步】按钮。

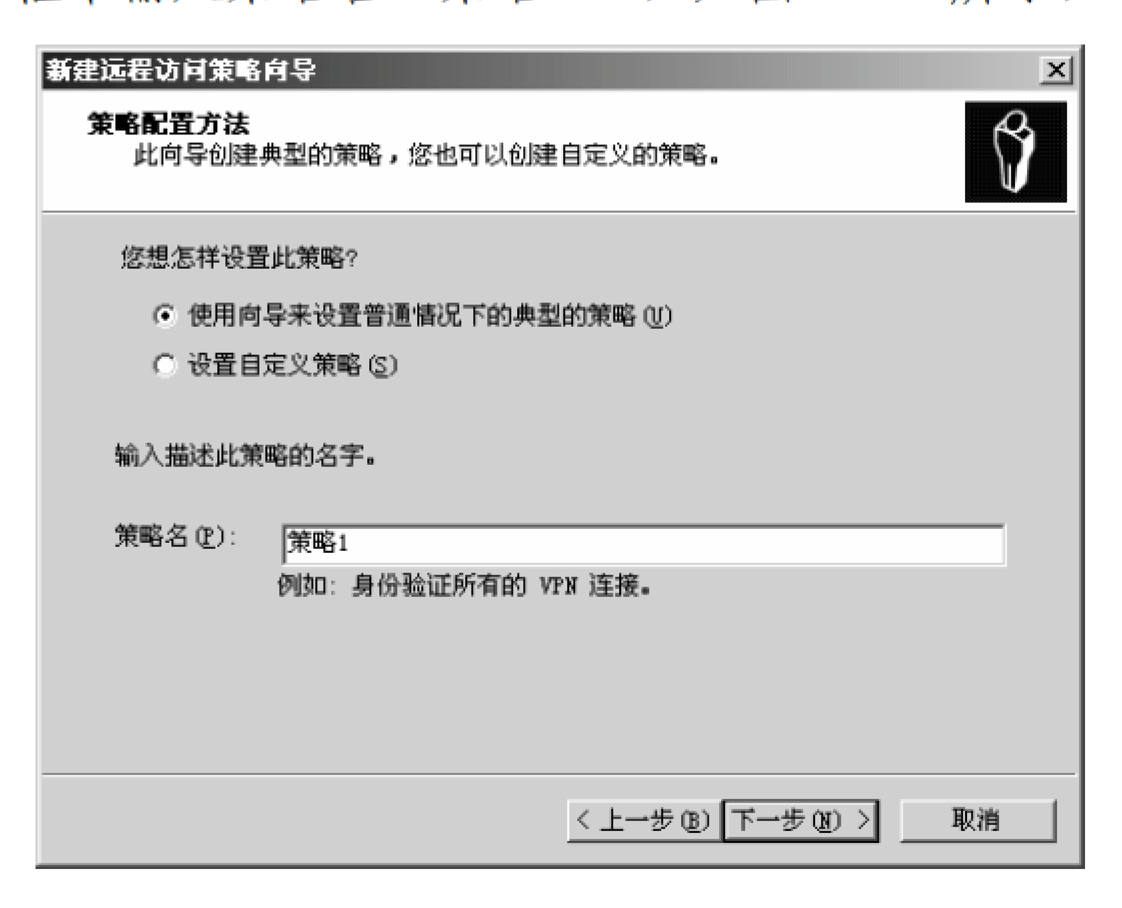


图 16-29

04 如图 16-30 所示，弹出【访问方法】对话框，选择策略应用于何种远程访问连接方式，选择【VPN】单选按钮，单击【下一步】按钮。

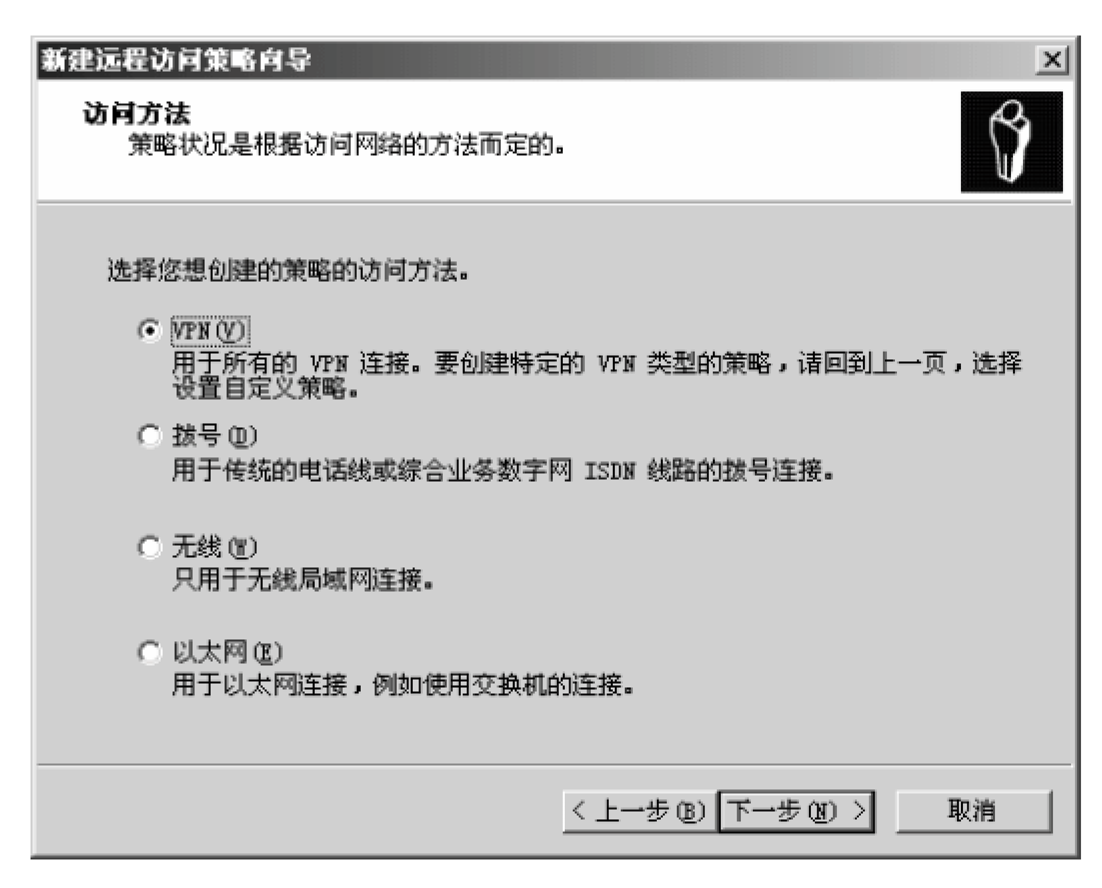


图 16-30

05 弹出【用户或组访问】对话框，在本地用户和组管理工具中可以设置用户或者组的远程访问权限，要和本步骤相对应，因为前面设置了“user1”用户的远程访问权限，所以选择【用户】单选按钮，如图 16-31 所示，单击【下一步】按钮。

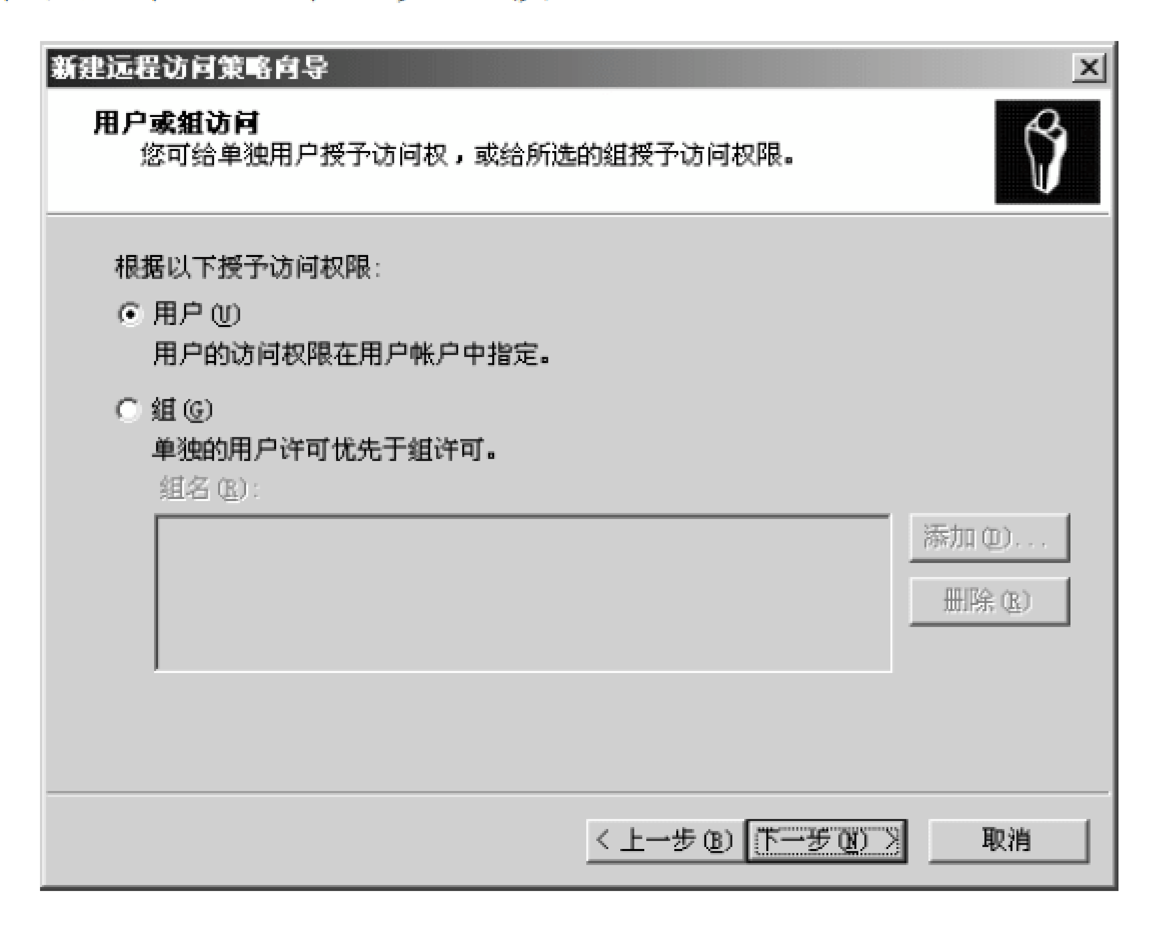


图 16-31

06 弹出【身份验证方法】对话框，如图 16-32 所示，选择远程访问 VPN 连接使用的身份验证方法，采用默认配置，单击【下一步】按钮。

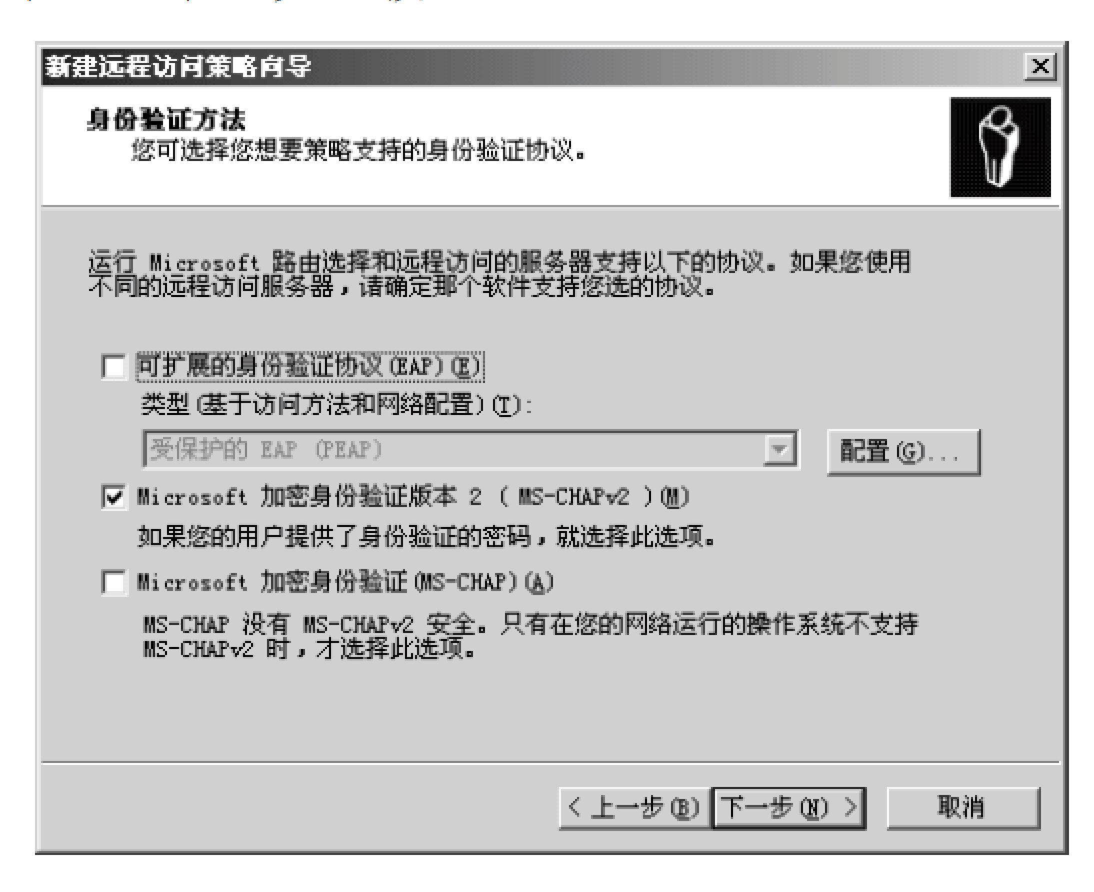


图 16-32

07 弹出【策略加密级别】对话框，如图 16-33 所示，设置本策略支持的加密级别，不同的远程访问服务器加密级别不同，默认全选，单击【下一步】按钮。

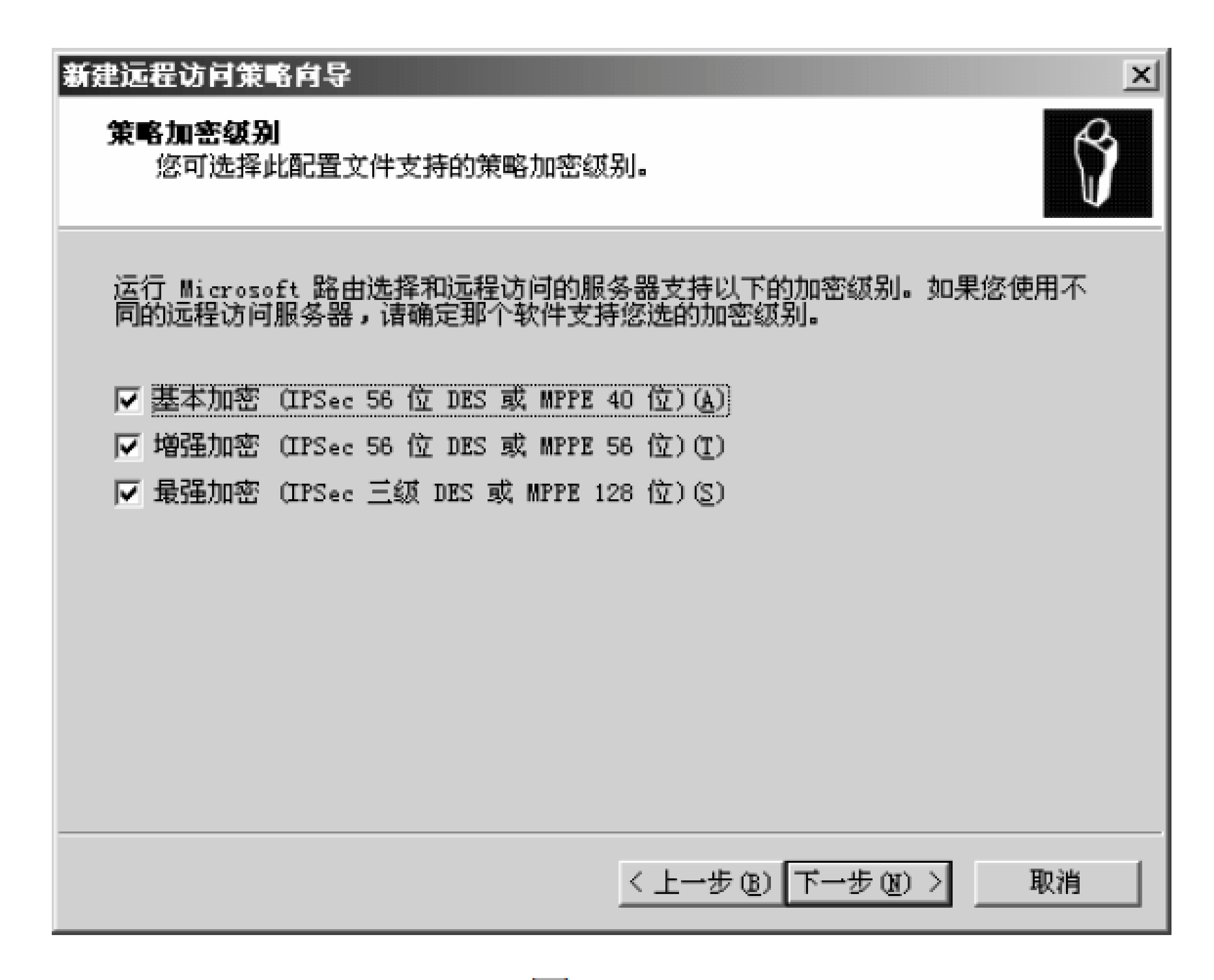


图 16-33

08 访问策略配置完成，显示出配置信息，单击【完成】按钮，如图 16-34 所示。

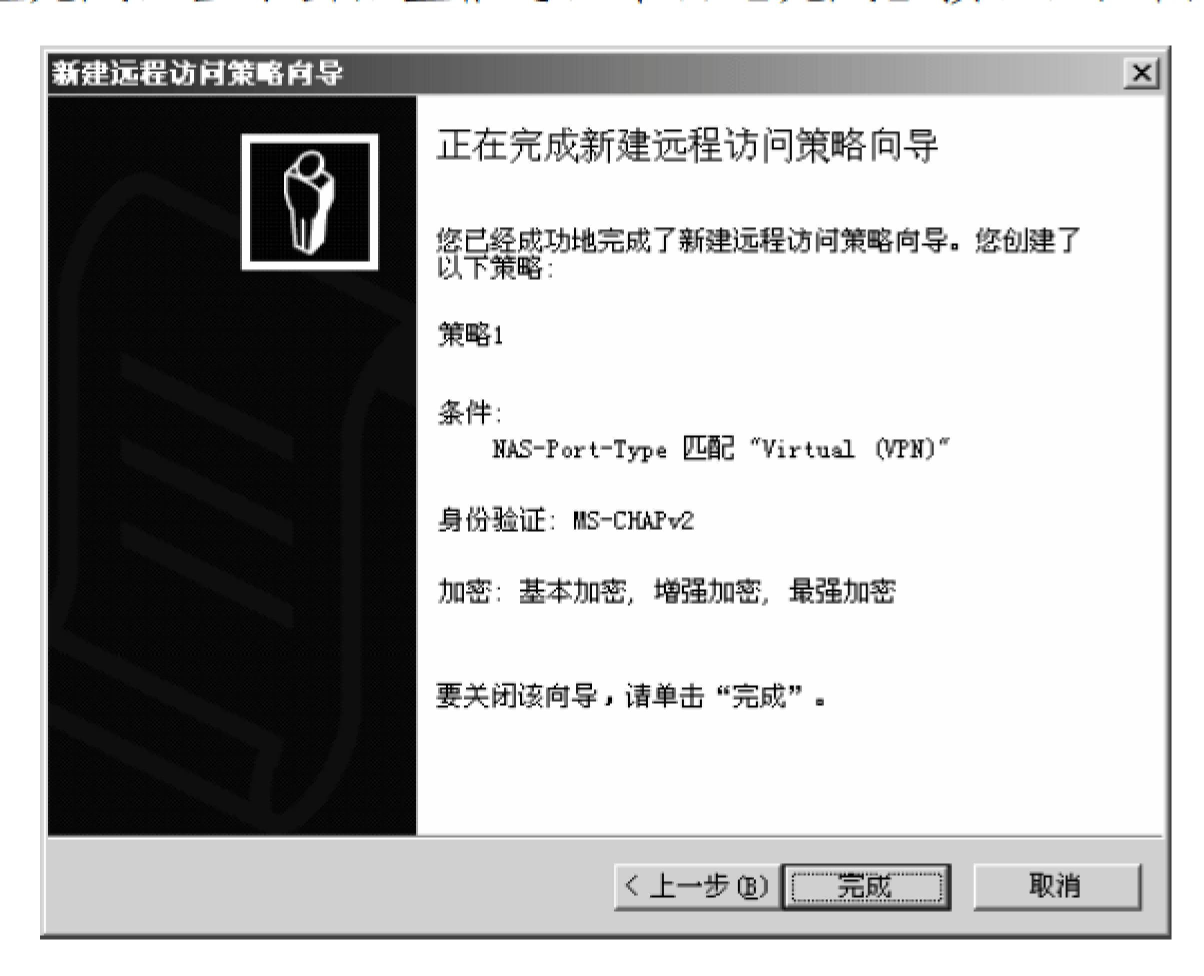


图 16-34

09 新策略添加成功，可以对策略进行配置，右击策略名，在弹出的快捷菜单中选择【属性】菜单命令，如图 16-35 所示。



图 16-35

10 弹出【策略 1 属性】对话框，如图 16-36 所示，在【策略状态】列表框中显示了默认的策略条目，单击【添加】按钮增加新策略。

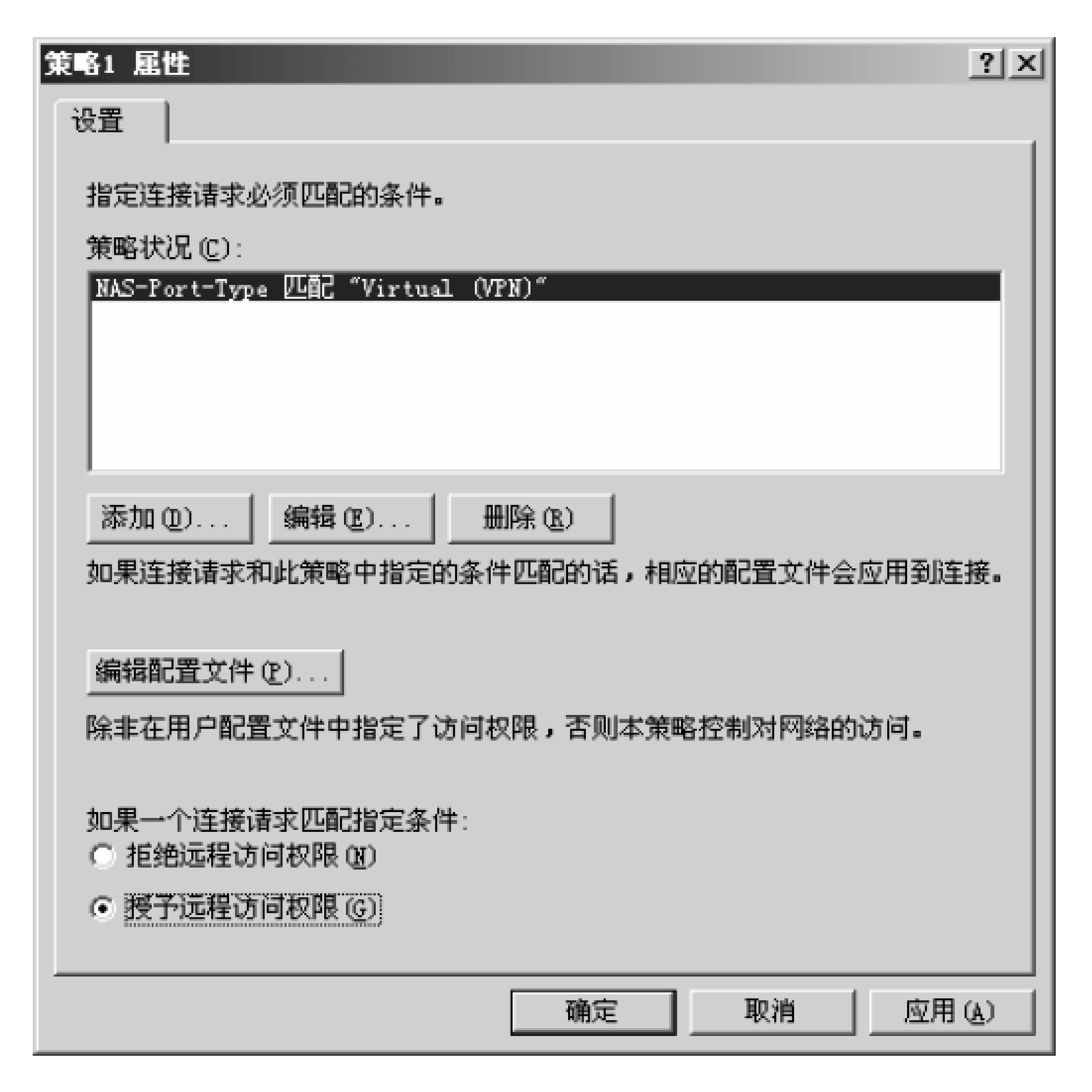


图 16-36

11 弹出【选择属性】对话框，在【属性类型】列表框中显示了可增加的策略类型，选择【Day-And-Time-Restrictions】选项，配置每周允许用户连接的时间和日期，单击【添加】按钮，如图 16-37 所示。

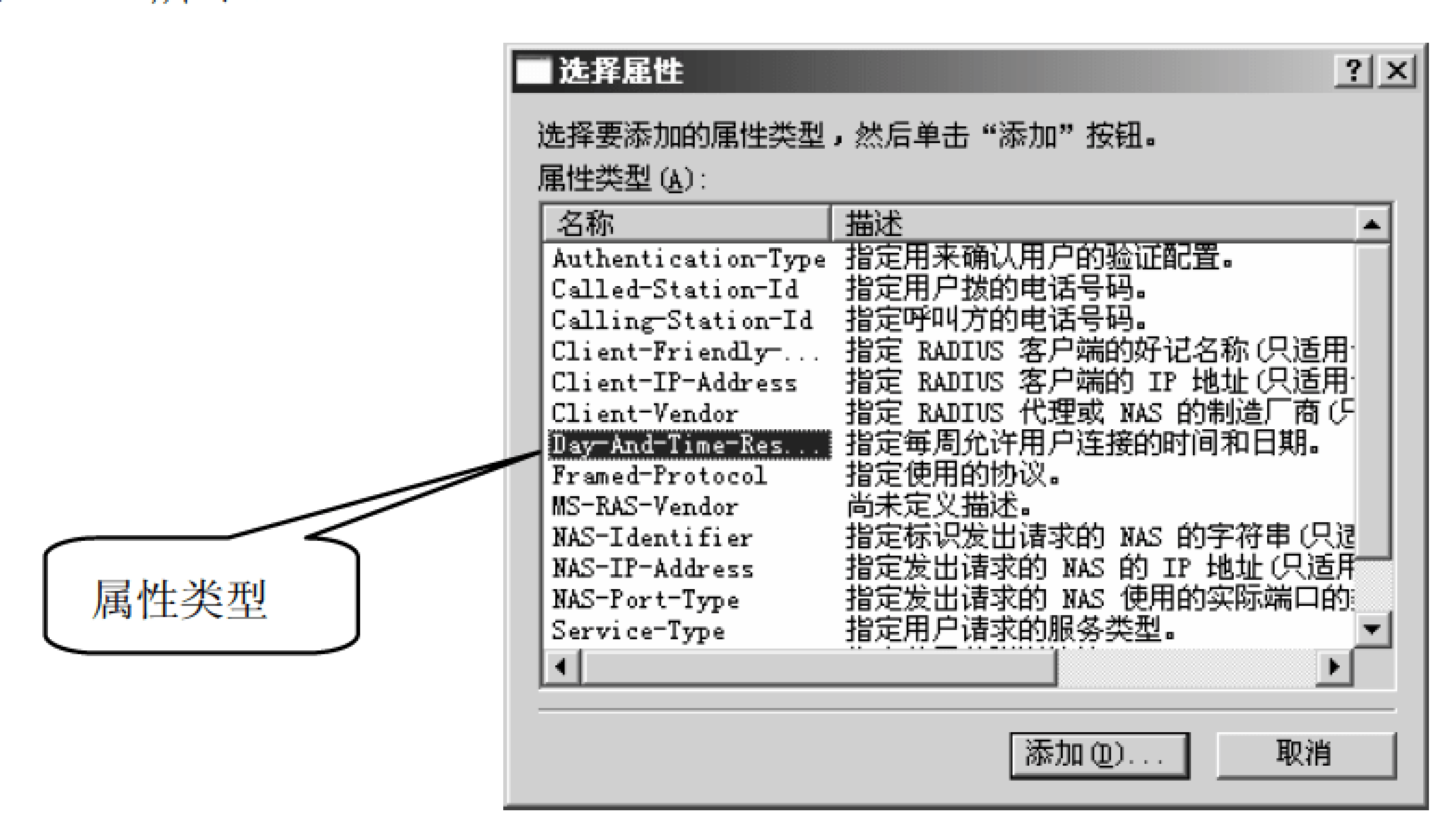


图 16-37

12 弹出【时间限制】对话框，单击鼠标左键拖选时间区域，选择【允许】单选按钮，如图 16-38 所示，单击【确定】按钮。

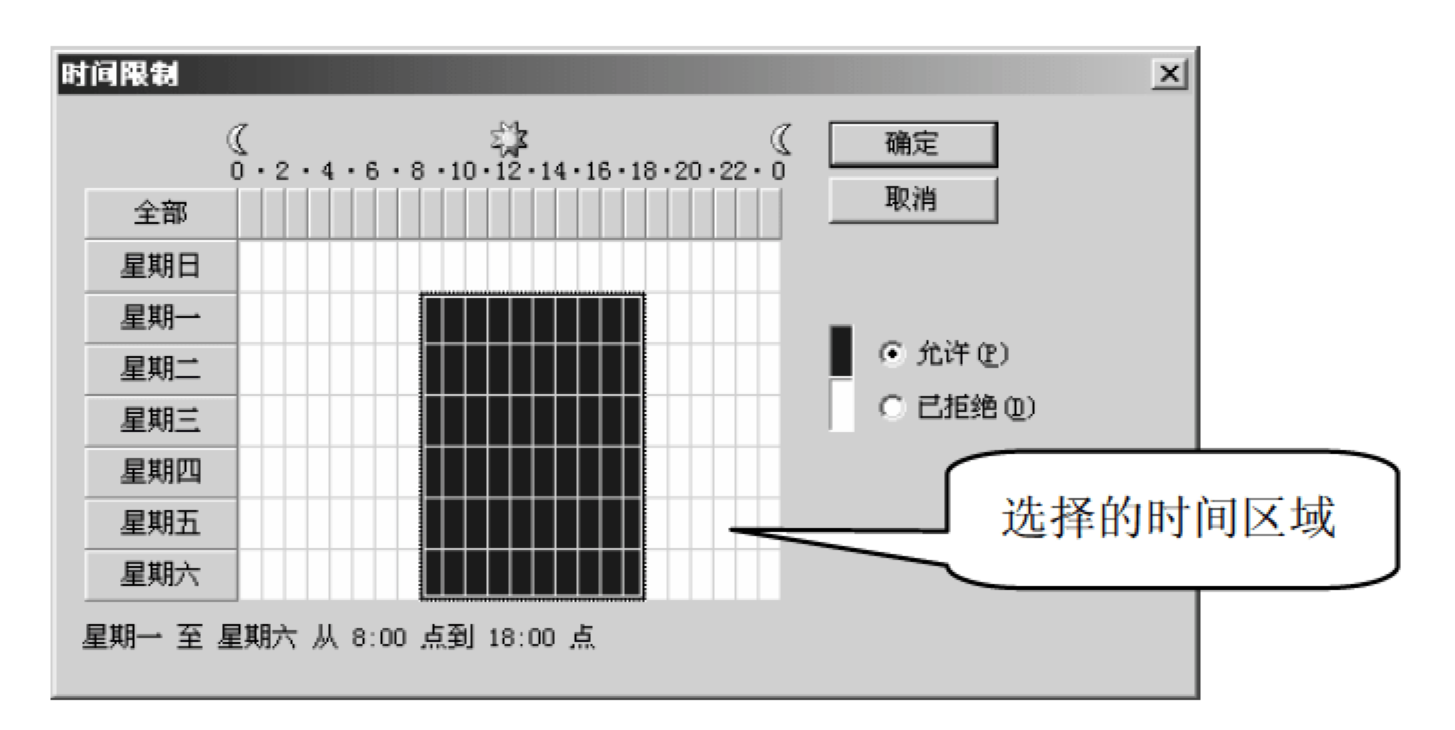


图 16-38

13 访问时间限制配置完成，返回【策略 1 属性】对话框，选择【授予远程访问权限】单选按钮，如图 16-39 所示，单击【确定】按钮，完成新策略的添加及属性修改。

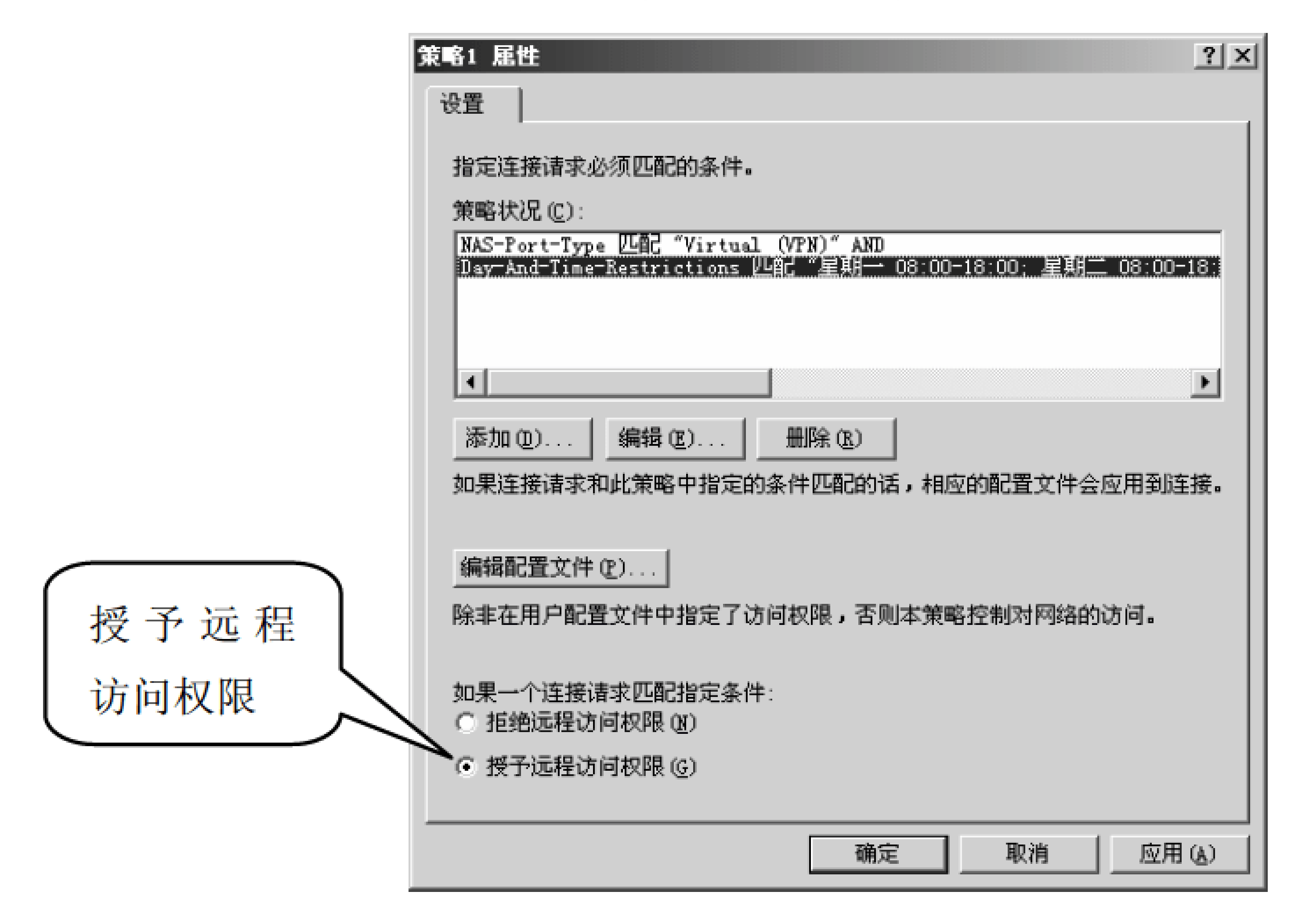


图 16-39

3. 客户端连接

设置客户端连接的具体操作步骤如下。

01 在远程客户端打开【网络连接】窗口，双击【新建连接向导】图标，如图 16-40 所示。



图 16-40

02 弹出【新建连接向导】对话框，单击【下一步】按钮，如图 16-41 所示。



图 16-41

03 弹出【网络连接类型】对话框，选择【连接到我的工作场所的网络】单选按钮，如图 16-42 所示，单击【下一步】按钮。

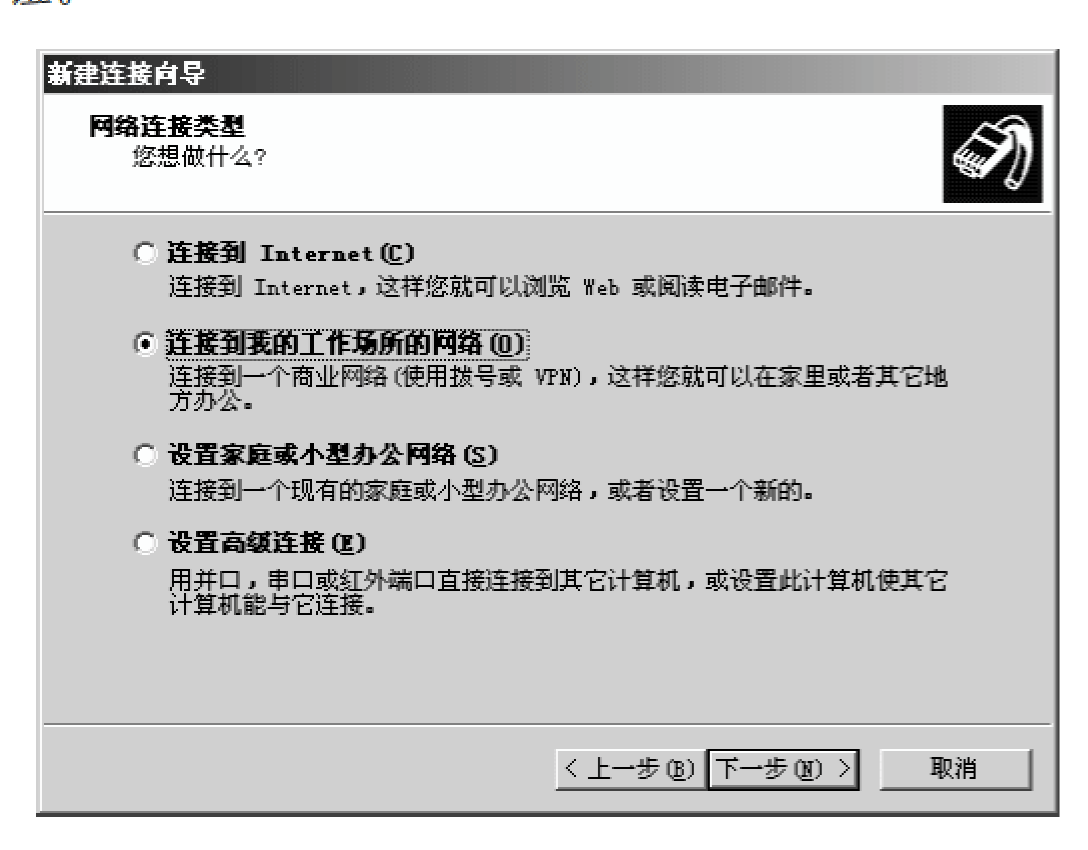


图 16-42

04 弹出【网络连接】对话框，选择【虚拟专用网络连接】单选按钮，如图 16-43 所示，单击【下一步】按钮。

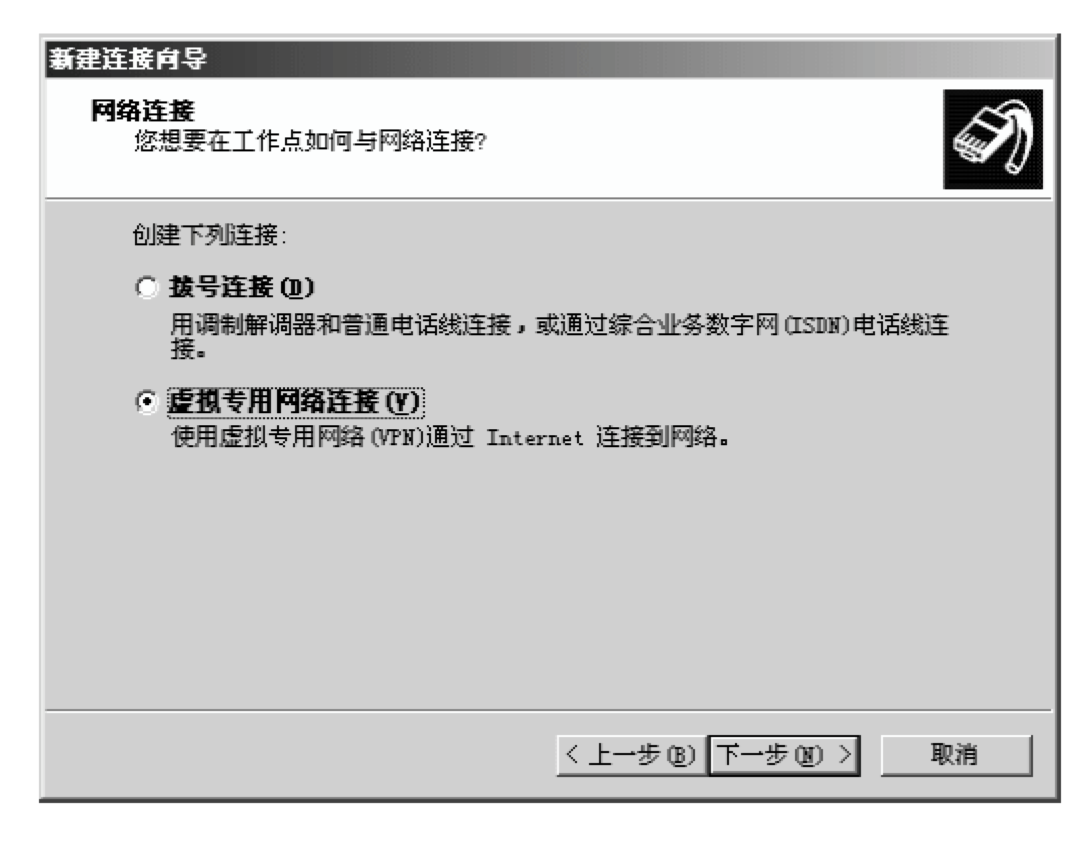


图 16-43

05 弹出【连接名】对话框，如图 16-44 所示，在【公司名】文本框中输入本次连接的名字“computerA”，为了方便记忆建议输入远程访问服务器所在公司名，单击【下一步】按钮。



图 16-44

06 弹出【VPN 服务器选择】对话框，在【主机名或 IP 地址】文本框输入远程访问服务器的地址，本实例为“61.192.93.100”，如图 16-45 所示，单击【下一步】按钮。

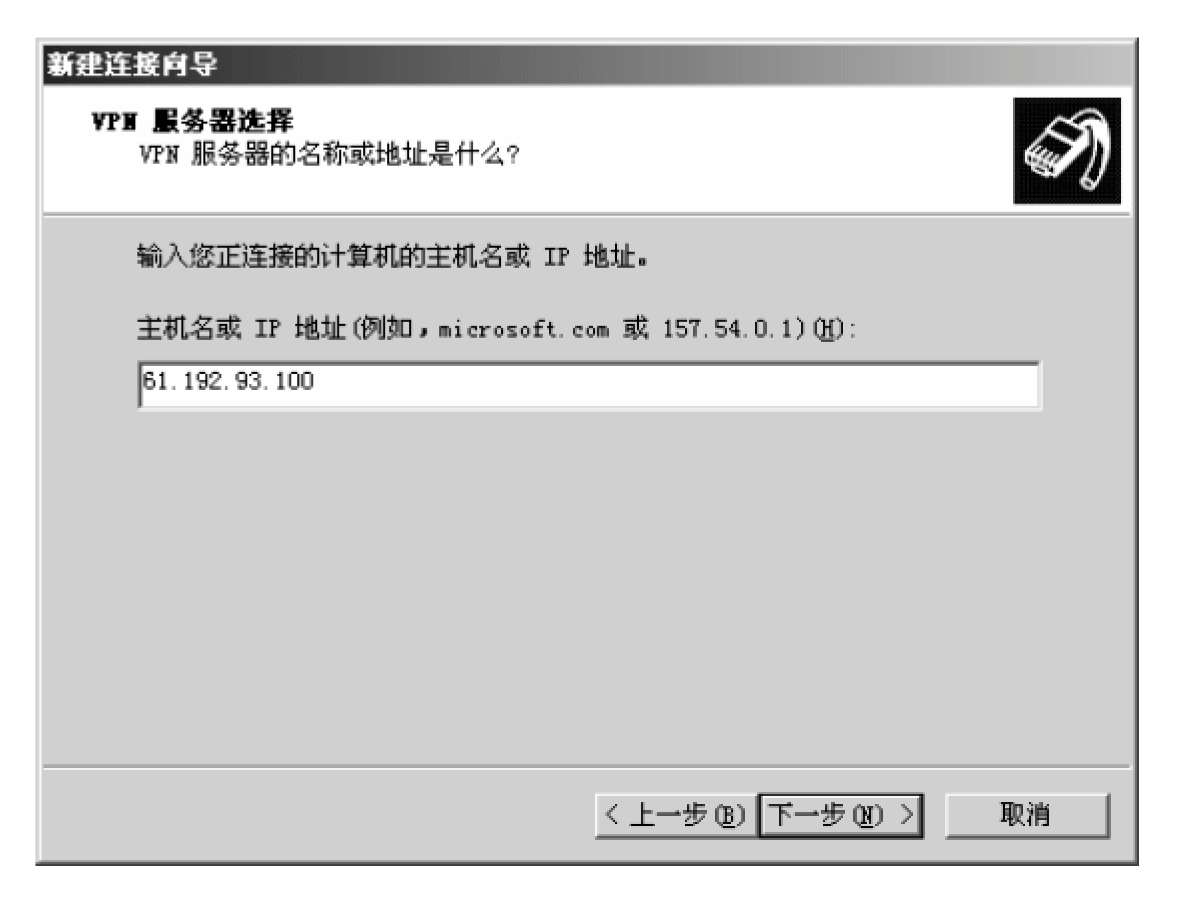


图 16-45

07 新建连接向导配置完成，为了方便连接，可以选择【在我的桌面上添加一个到此连接的快捷方式】单选按钮，如图 16-46 所示，单击【下一步】按钮。



图 16-46

08 弹出【连接 computerA】对话框，在【用户名】和【密码】文本框输入进行身份认证的账户及密码信息，如图 16-47 所示，单击【连接】按钮。



图 16-47

09 自动认证连接，并从远程访问服务器获得 IP 地址，添加成功后会在【网络连接】窗口显示连接图标，如图 16-48 所示。



图 16-48

10 右击连接图标，选择【状态】菜单命令，弹出【computerA 状态】对话框，如图 16-49 所示，在【常规】选项卡中显示了连接状态，【活动】状态信息中的【压缩】状态表示信息使用 VPN 连接发送时的压缩比例，默认使用 VPN 传输的数据都进行了压缩。

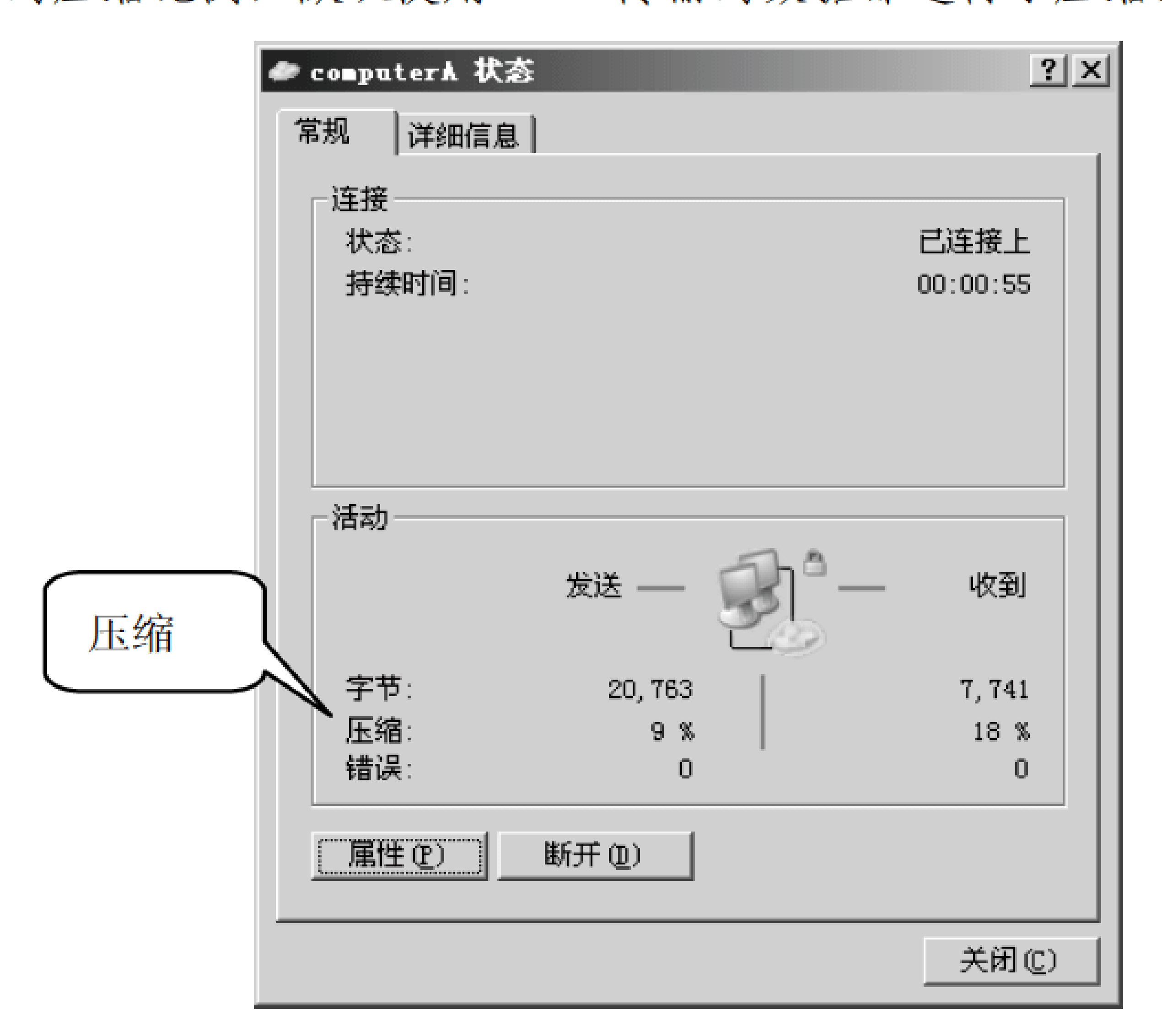


图 16-49

11 如图 16-50 所示，在【详细信息】选项卡中显示了客户端用于连接远程访问服务器的信息，包括：压缩方式、加密方式、身份验证方式、远程服务器地址、客户端地址等信息。

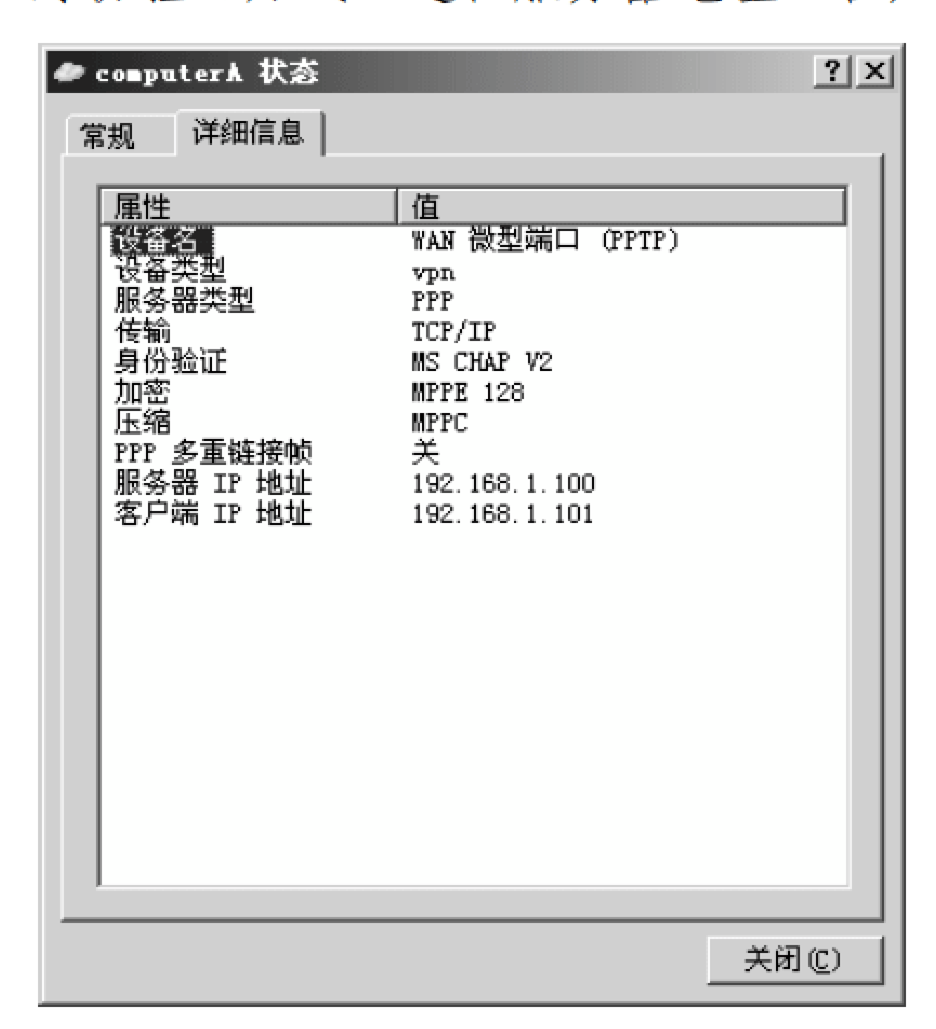


图 16-50

16.3 基于 ISA 防火墙的 VPN

ISA Server 2006 防火墙本身自带有 VPN 配置功能，可以实现远程访问 VPN 和 IPSec VPN 两

种技术。

16.3.1　远程访问 VPN

远程访问 VPN 可以按照如图 16-51 所示的拓扑图实现方案配置，具体的配置步骤如下。

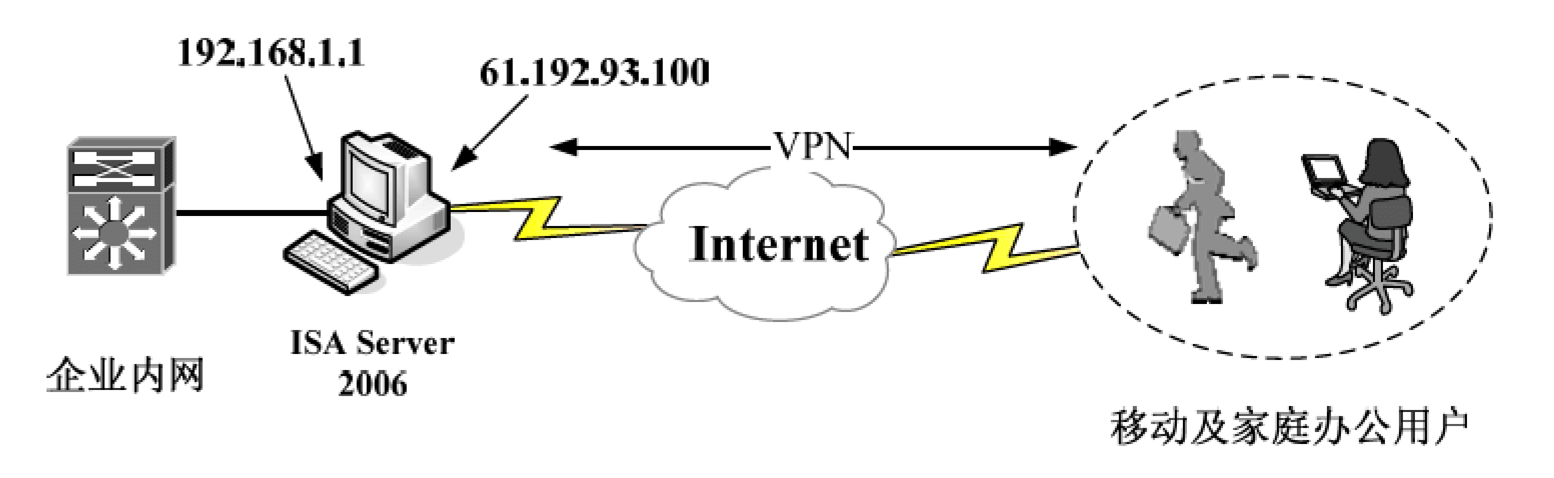


图 16-51

1. 定义远程客户端地址段

具体的操作步骤如下。

01 打开 ISA Server 2006 程序主界面，如图 16-52 所示，在左侧选项列表中选择【虚拟专用网（VPN）】选项，选择【VPN 客户端】选项卡，选择右侧【任务】选项卡的【定义地址分配】选项。



图 16-52

02 弹出【虚拟专用网（VPN）属性】对话框，如图 16-53 所示，单击【添加】按钮，为远程客户端指定可分配的地址。

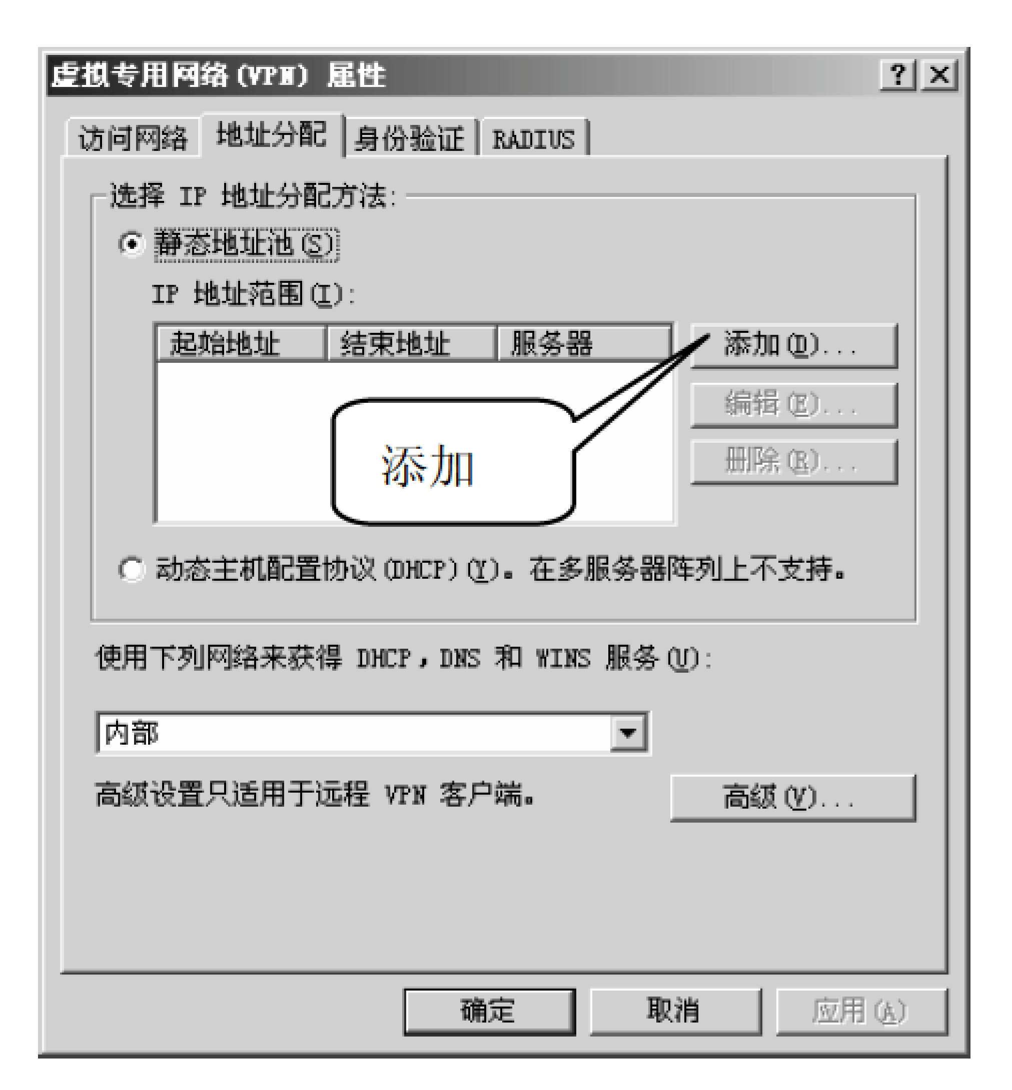


图 16-53

03 弹出【服务器 IP 地址范围属性】对话框，如图 16-54 所示，在【起始地址】和【结束地址】文本框中输入地址范围，单击【确定】按钮。

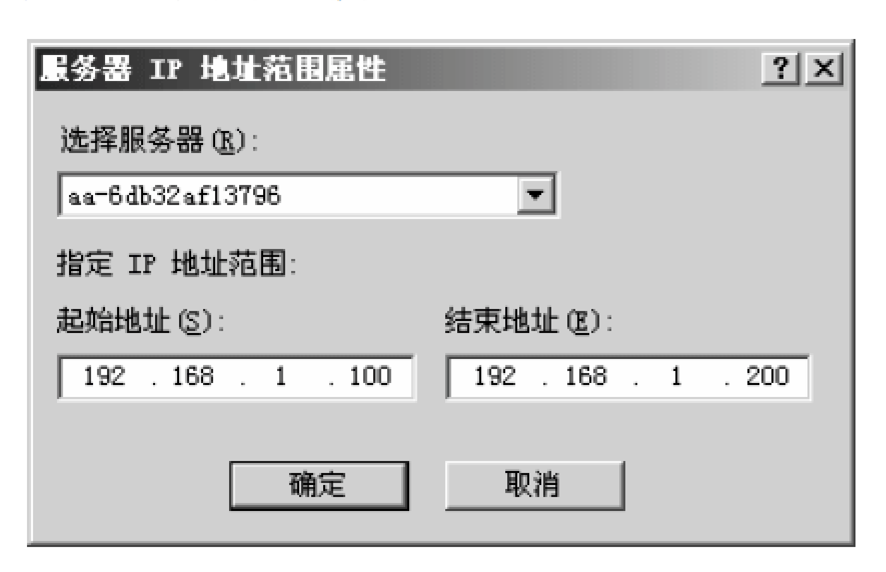


图 16-54

04 返回【虚拟专用网（VPN）属性】对话框，如图 16-55 所示，选择【访问网络】选项卡，勾选【外部】复选框，指定该地址配置应用于外部网络的客户机。

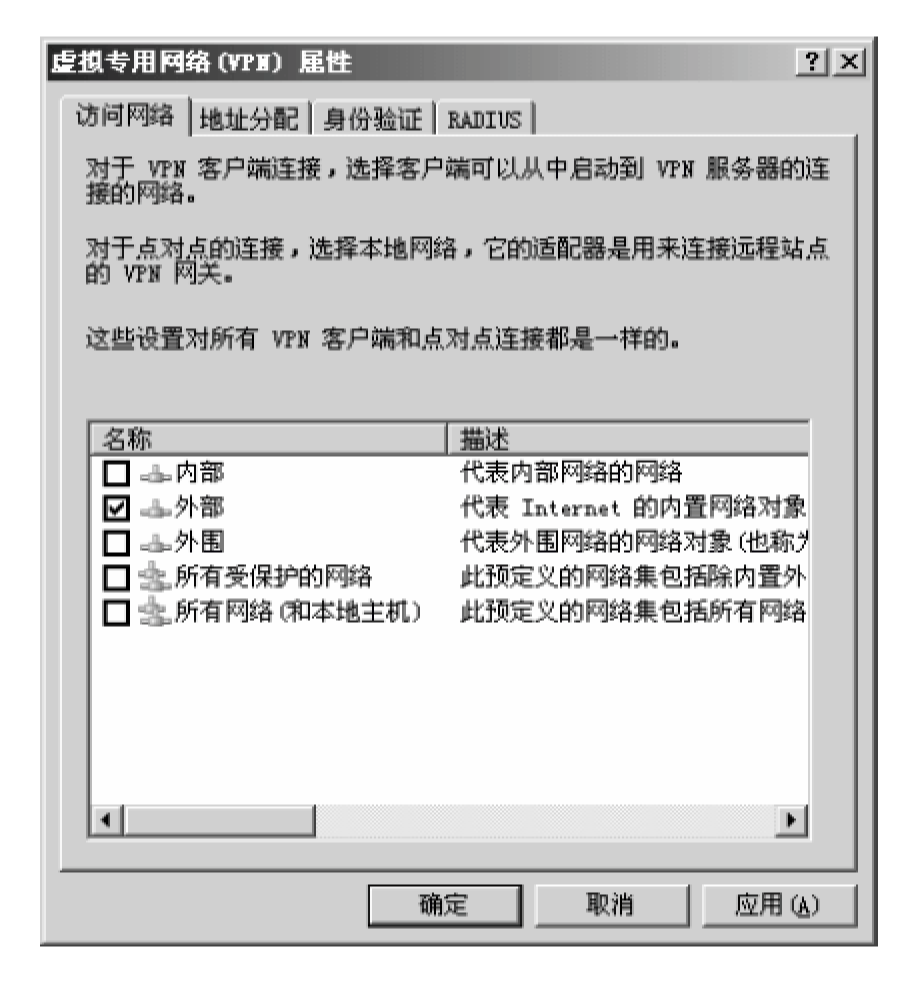


图 16-55

05 如图 16-56 所示，选择【身份验证】选项卡，指定客户端连接使用的身份验证方式，默认为“MS-CHAPv2”认证技术，单击【确定】按钮。

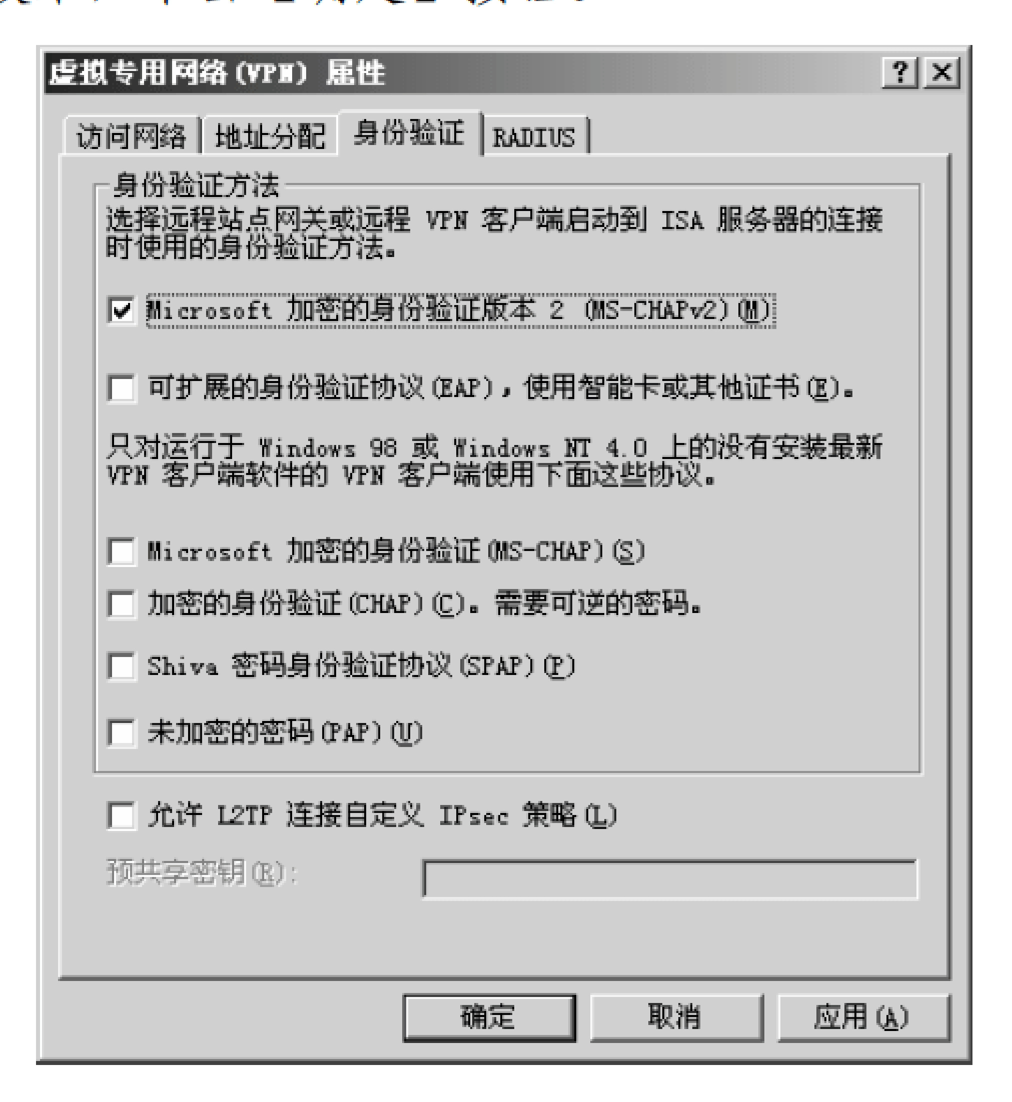


图 16-56

2. 配置 VPN 客户端访问

具体的操作步骤如下。

01 打开 ISA Server 2006 程序主界面，如图 16-57 所示，在左侧选项列表中选择【虚拟专用网（VPN）】选项，选择【VPN 客户端】选项卡，选择右侧【任务】选项卡的【配置 VPN 客户端访问】选项。



图 16-57

02 弹出【VPN 客户端 属性】对话框，选择【常规】选项卡，如图 16-58 所示，勾选【启用 VPN 客户端访问】复选框，在【允许的最大 VPN 客户端数量】文本框中默认显示“100”，可根据企业需求调整。

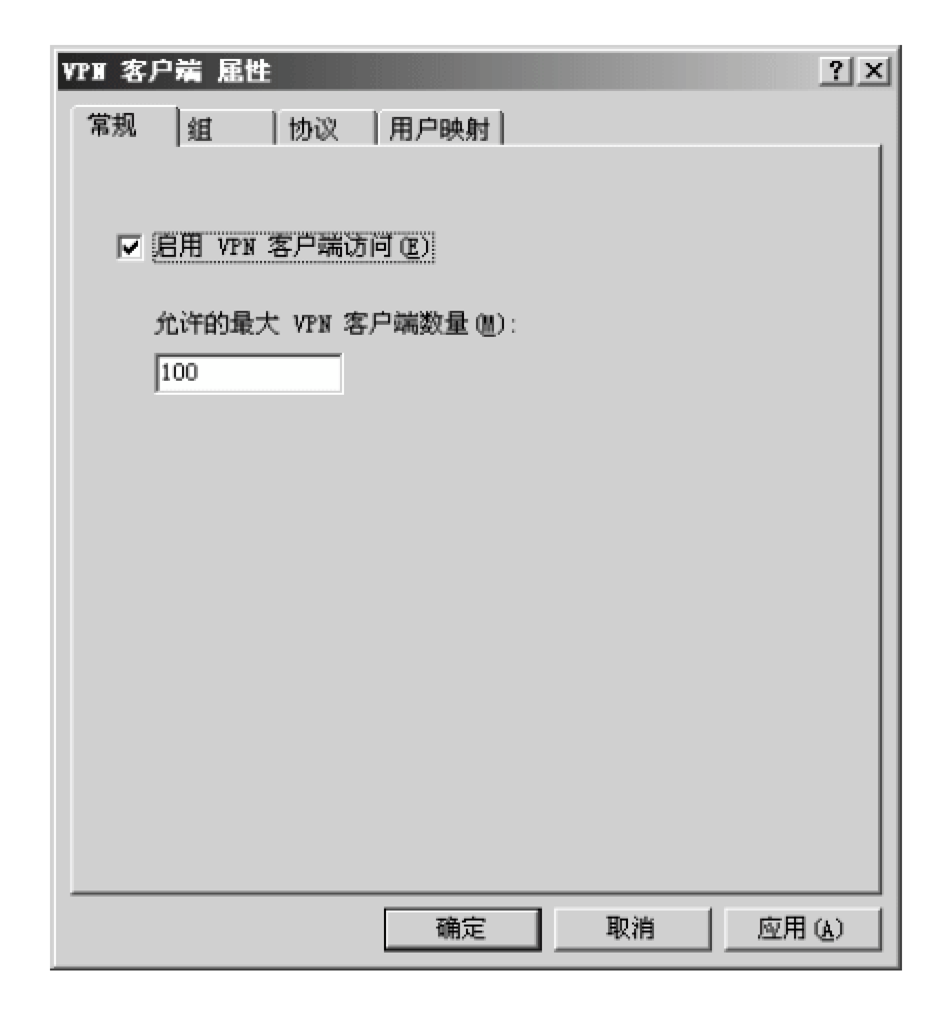


图 16-58

03 如图 16-59 所示，选择【组】选项卡，可以通过单击【添加】按钮配置允许访问的远程域组，本实例没有使用域，不做配置。

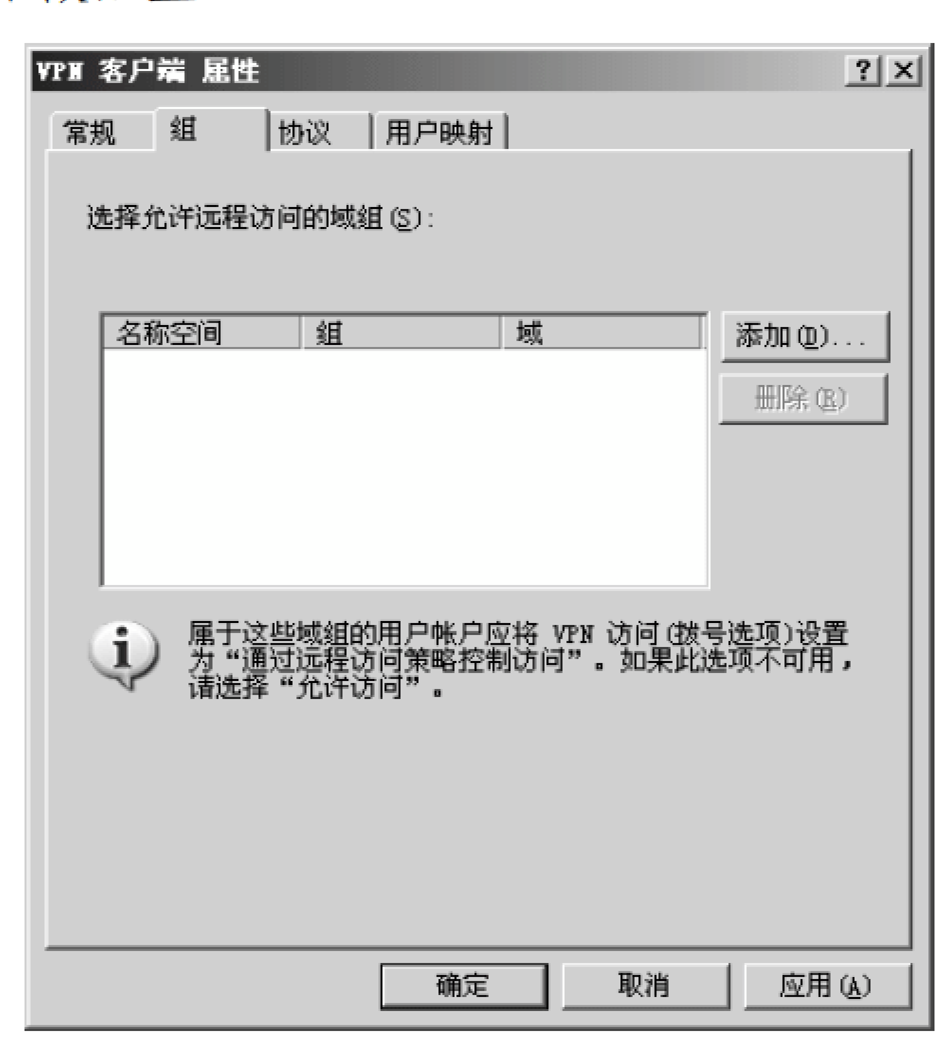


图 16-59

04 如图 16-60 所示，选择【协议】选项卡，选择 VPN 连接使用的协议，默认选择【启用 PPTP】复选框，本实例不采用认证技术，所以不选择【启用 L2TP/IPsec】复选框，单击【确定】按钮。

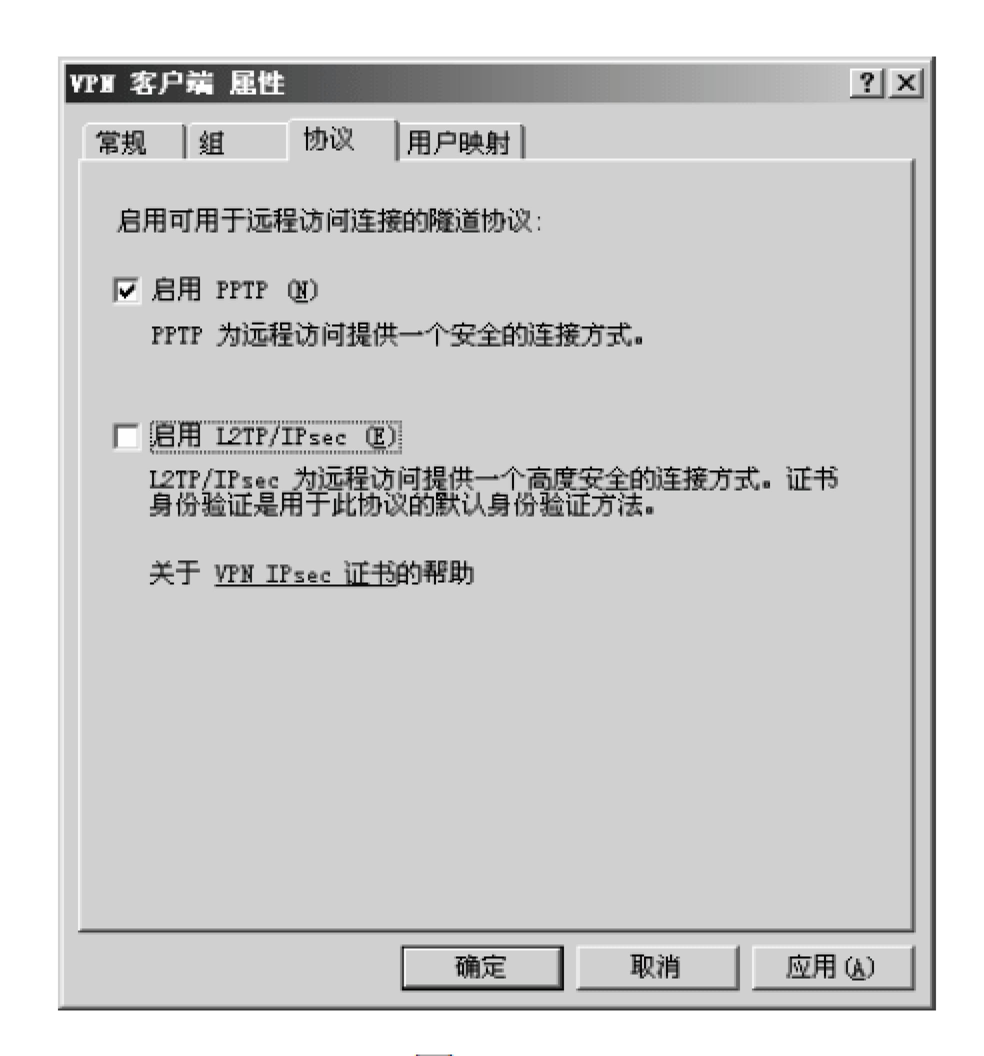


图 16-60



提 示

如果选择【启用 L2TP/IPsec】选项，就需要用到证书服务器，用户可以根据个人需求调整。

3.开放 VPN 客户端访问

VPN 连接配置完成后，如果允许 VPN 客户端和内网通信，需要创建一条访问规则，具体的操作步骤如下。

01 打开【新建访问规则向导】对话框，如图 16-61 所示，在【访问规则名称】文本框中输入“开放 VPN 客户端与内网通信”，单击【下一步】按钮。

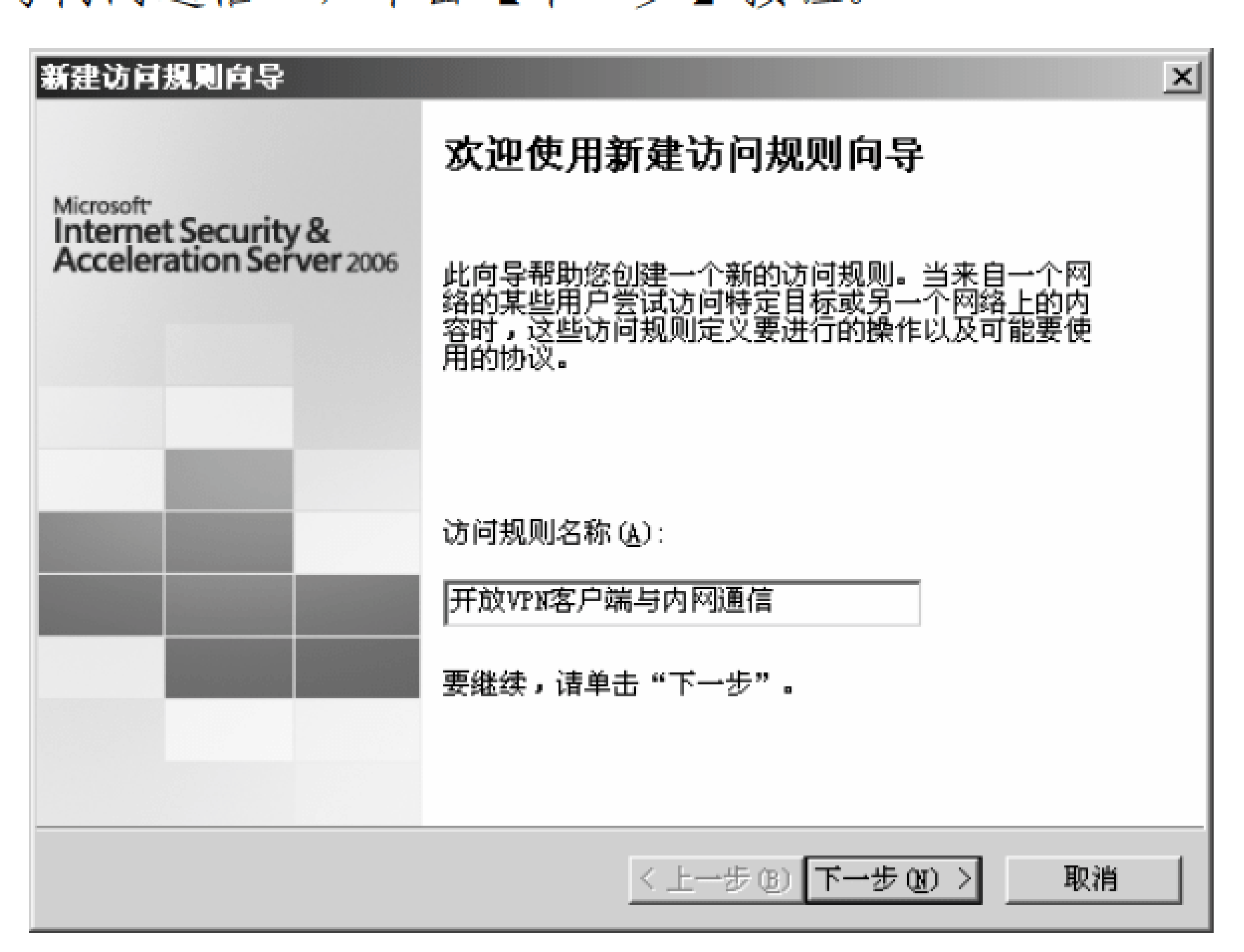


图 16-61

02 弹出【规则操作】对话框，选择【允许】单选按钮，单击【下一步】按钮，如图 16-62 所示。

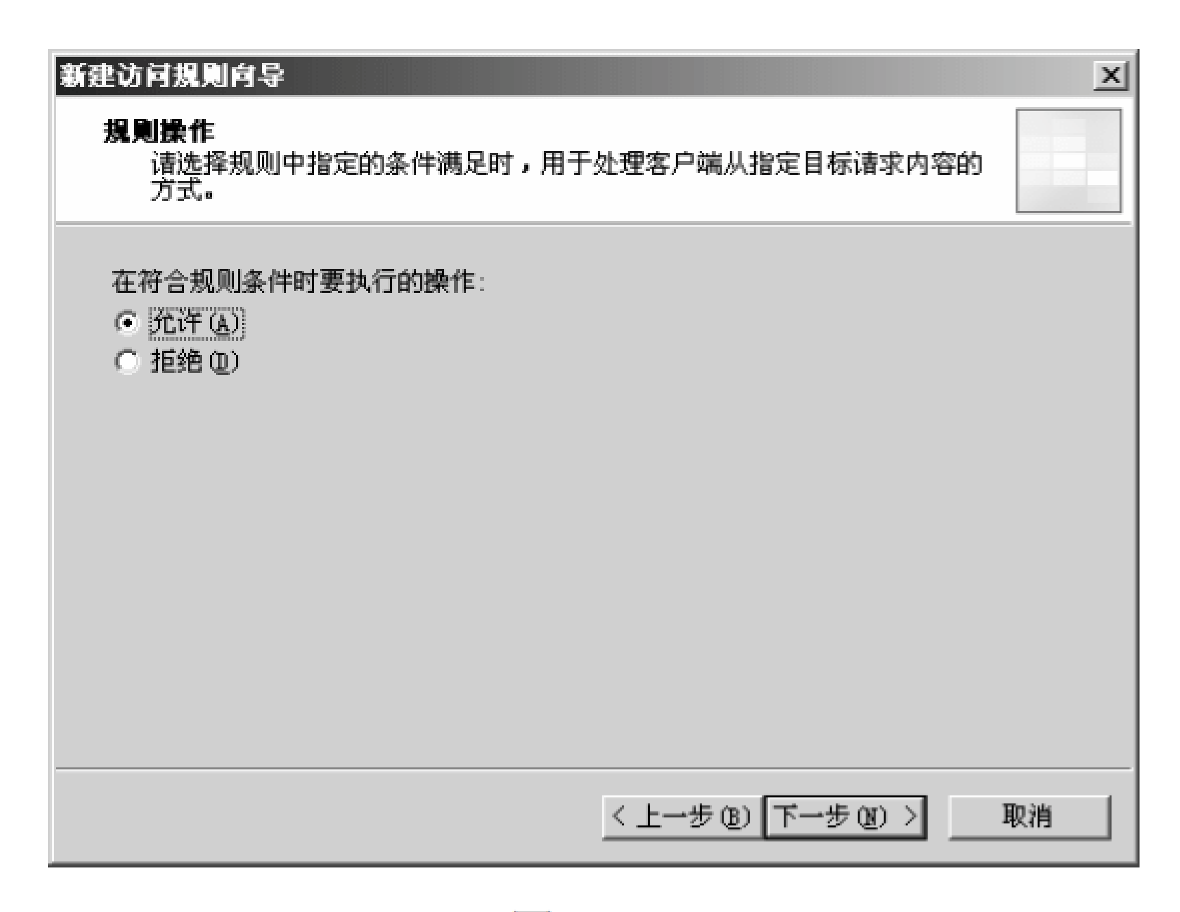


图 16-62

03 弹出【协议】对话框，如图 16-63 所示，在【此规则应用到】下拉菜单选项中选择【所有出站通信】选项，单击【下一步】按钮。



图 16-63

04 弹出【访问规则源】对话框，如图 16-64 所示，单击【添加】按钮，增加新访问源。

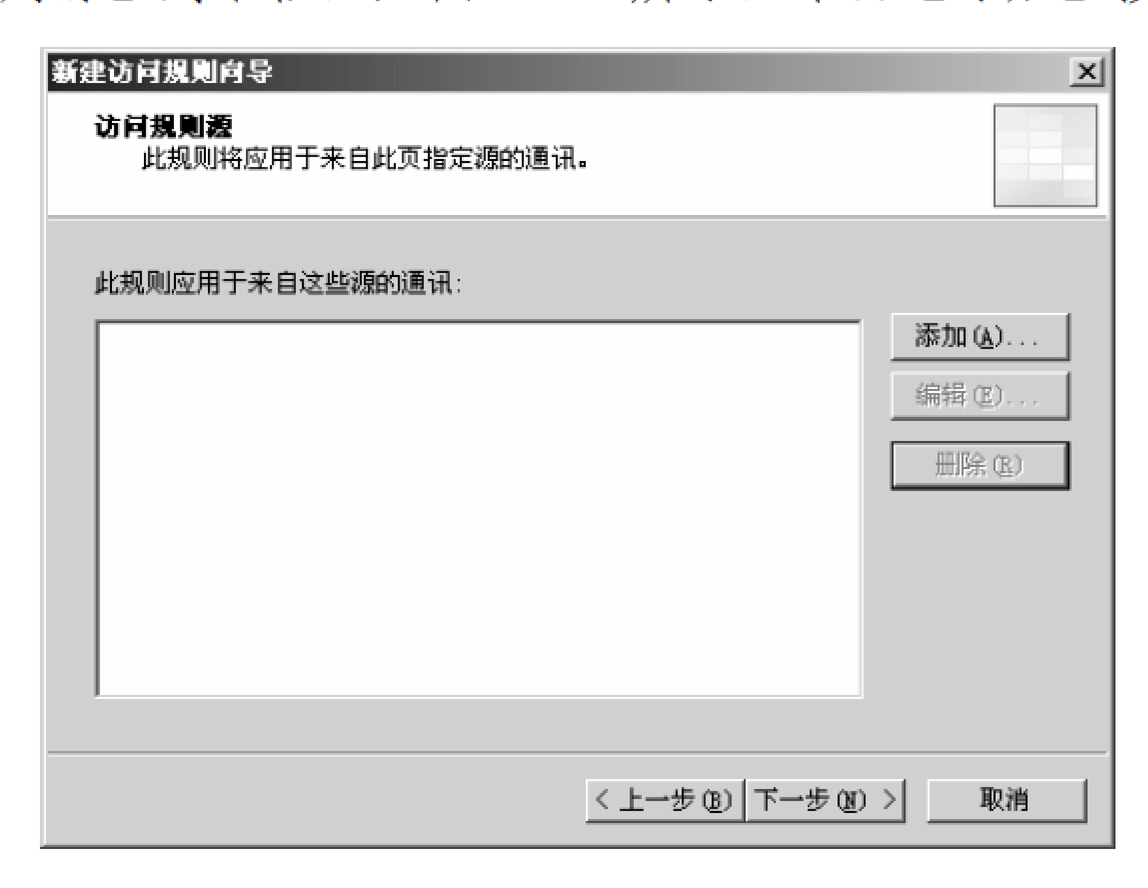


图 16-64

05 弹出【添加网络实体】对话框，如图 16-65 所示，在【网络】子选项中选择【VPN 客户

端】和【内部】两个选项，单击【关闭】按钮。



图 16-65

06 返回【访问规则源】对话框，访问源添加成功，单击【下一步】按钮，如图 16-66 所示。

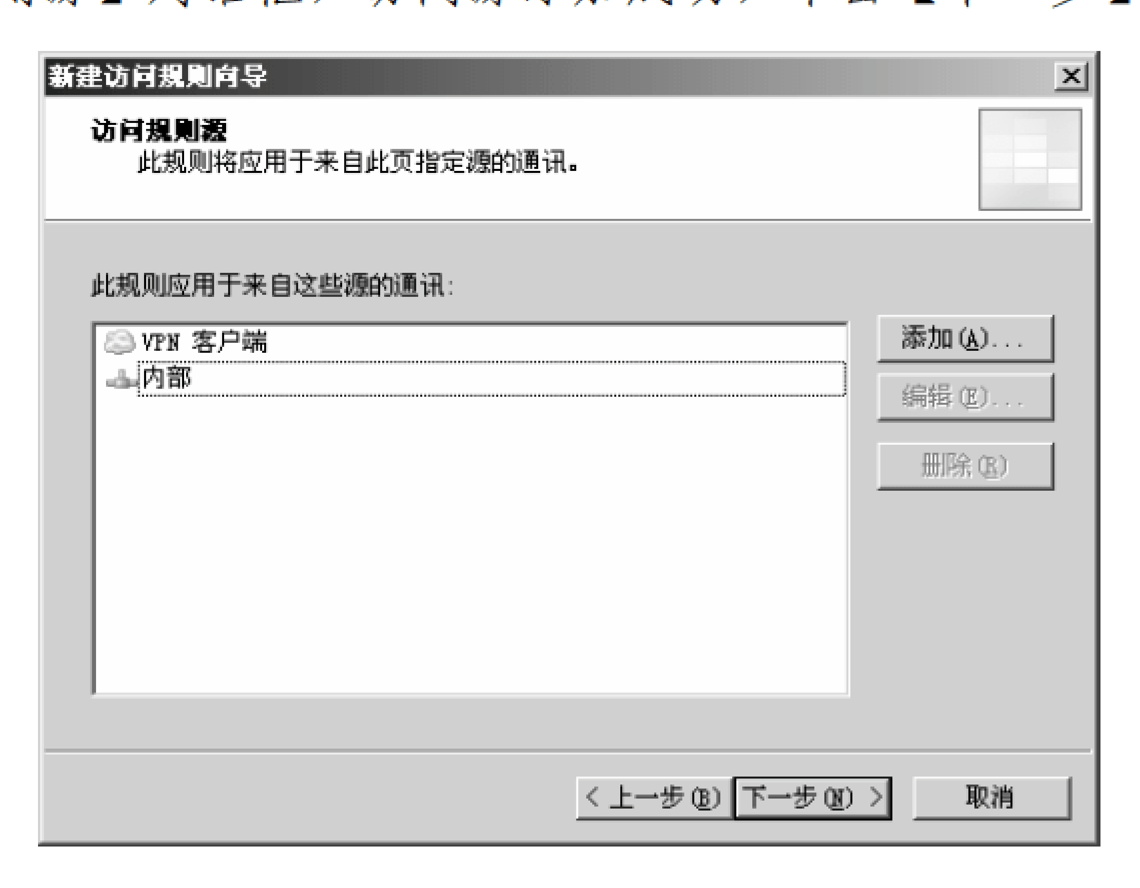


图 16-66

07 弹出【访问规则目标】对话框，如图 16-67 所示，依然添加【VPN 客户端】和【内部】两项，单击【下一步】按钮。

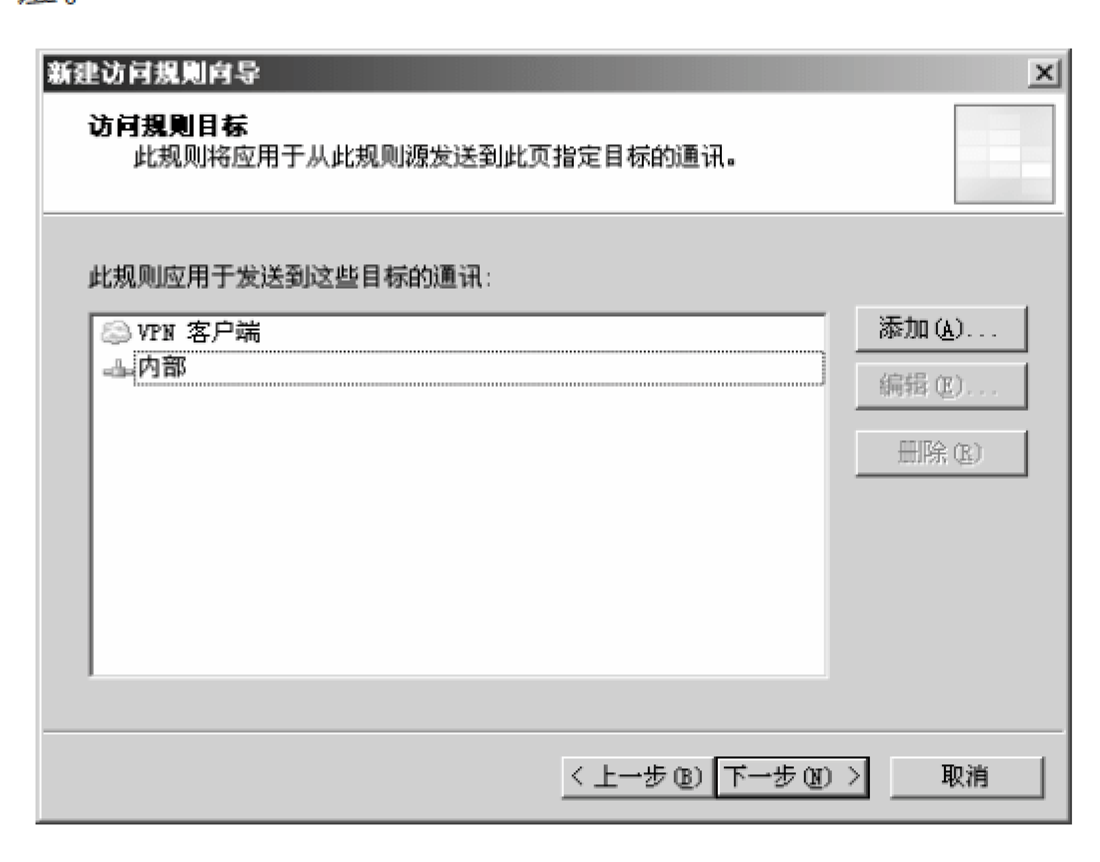


图 16-67

08 弹出【用户集】对话框，默认允许所有用户访问，单击【下一步】按钮，如图 16-68 所示。

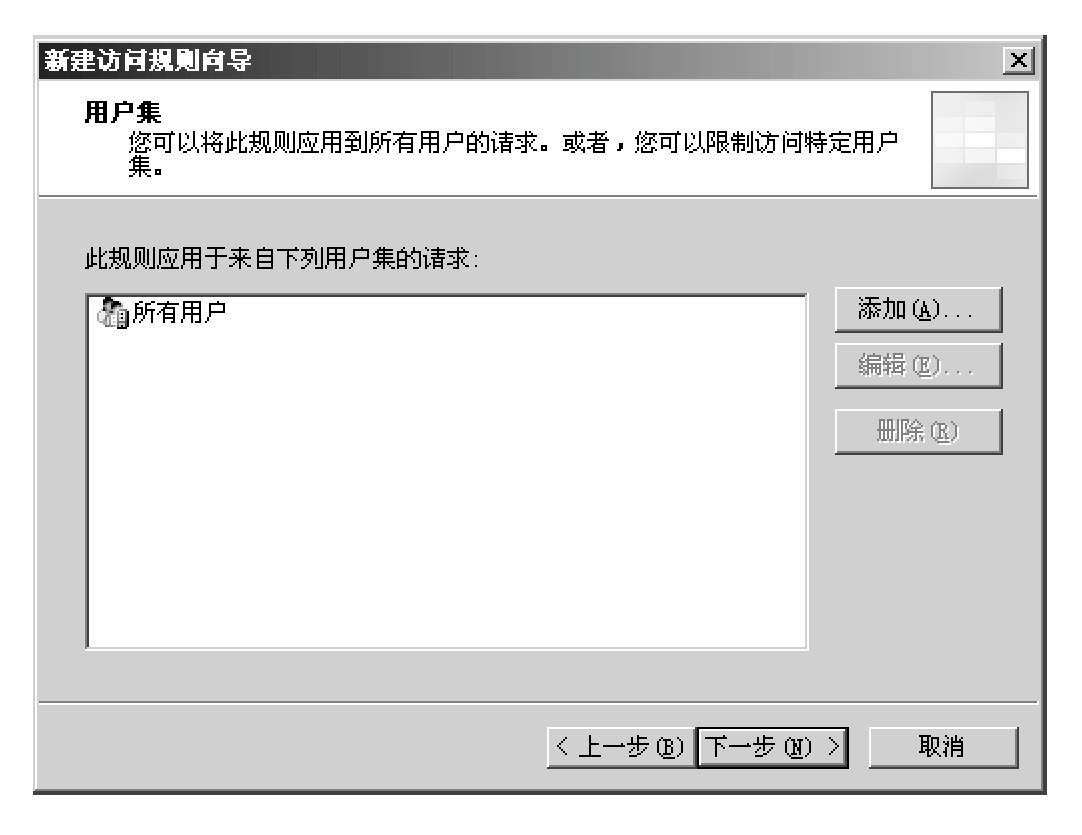


图 16-68

09 访问规则配置完成，显示出配置信息，单击【完成】按钮，完成向导，如图 16-69 所示。

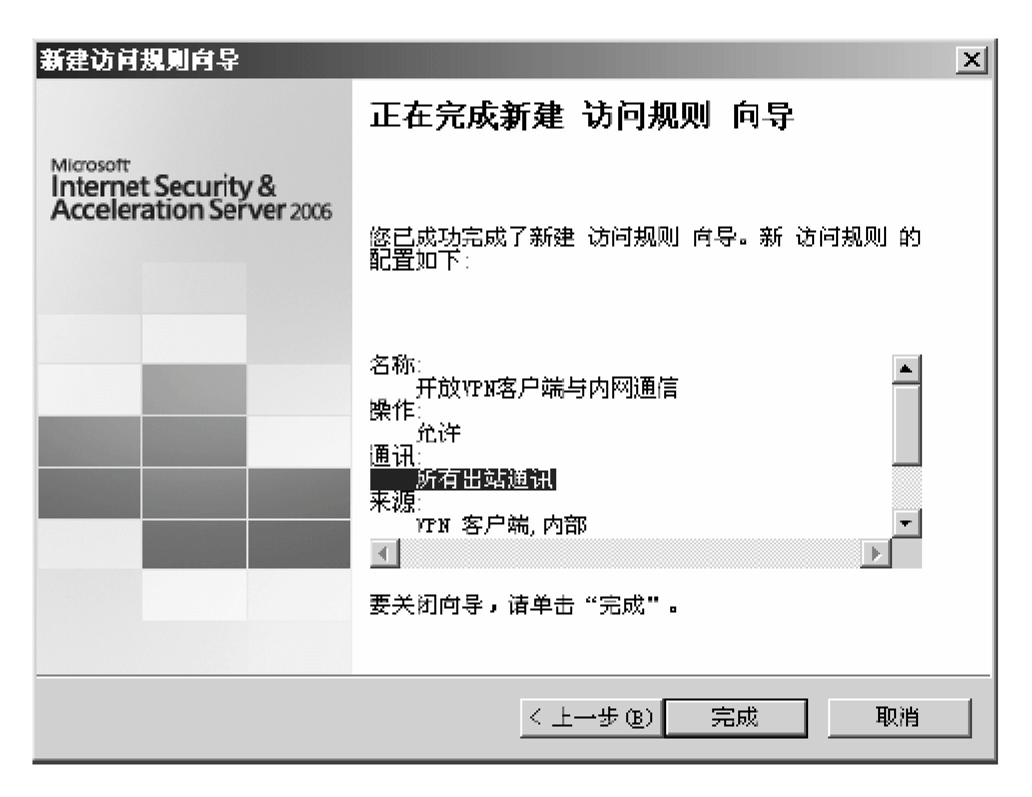


图 16-69

10 新规则添加成功，在【防火墙策略规则】列表中显示，单击【应用】按钮使配置生效，如图 16-70 所示。

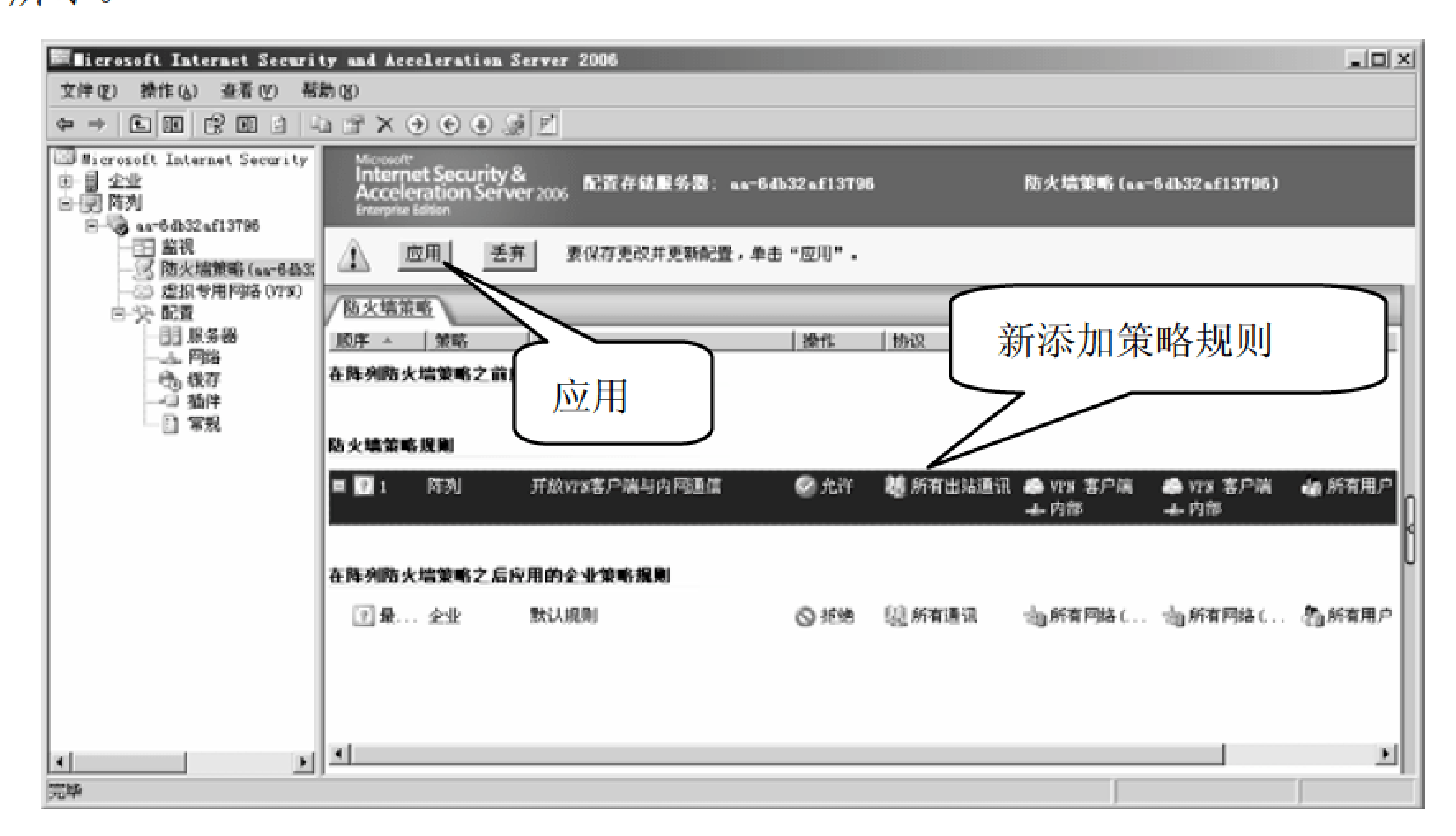


图 16-70

4. 配置身份认证用户

在 ISA 服务器的本地用户中找到有远程访问登录权限的账户，配置其属性，如图 16-71 所示，在【拨入】选项卡中，选择【允许访问】单选按钮，单击【确定】按钮。

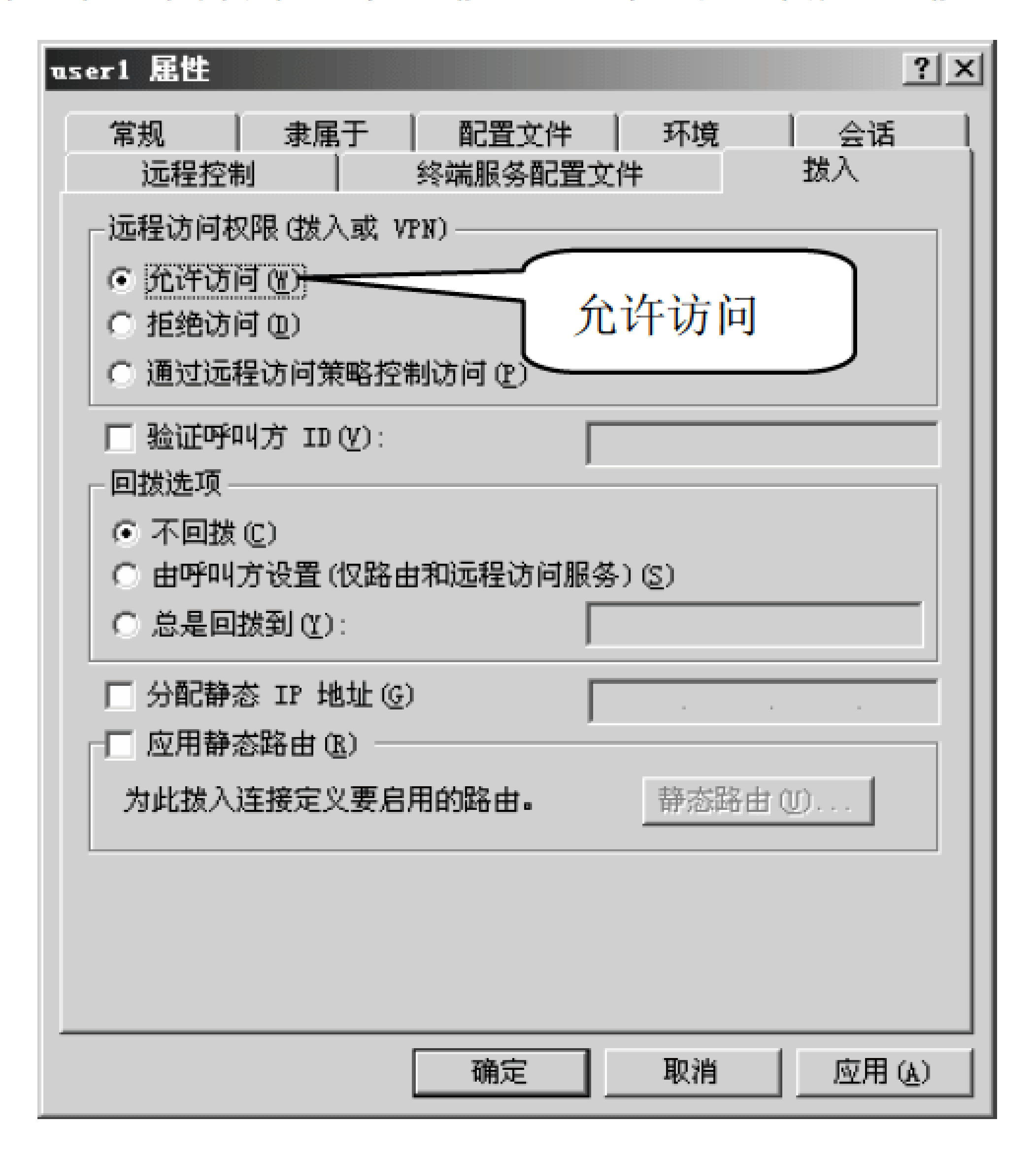


图 16-71

5. 客户端连接

配置方案的最后一步就是客户端连接，具体的操作步骤如下。

01 在远程客户端打开【网络连接】窗口，双击【新建连接向导】图标，如图 16-72 所示。



图 16-72

02 弹出【新建连接向导】对话框，单击【下一步】按钮，如图 16-73 所示。



图 16-73

03 弹出【网络连接类型】对话框，选择【连接到我的工作场所的网络】单选按钮，如图 16-74 所示，单击【下一步】按钮。

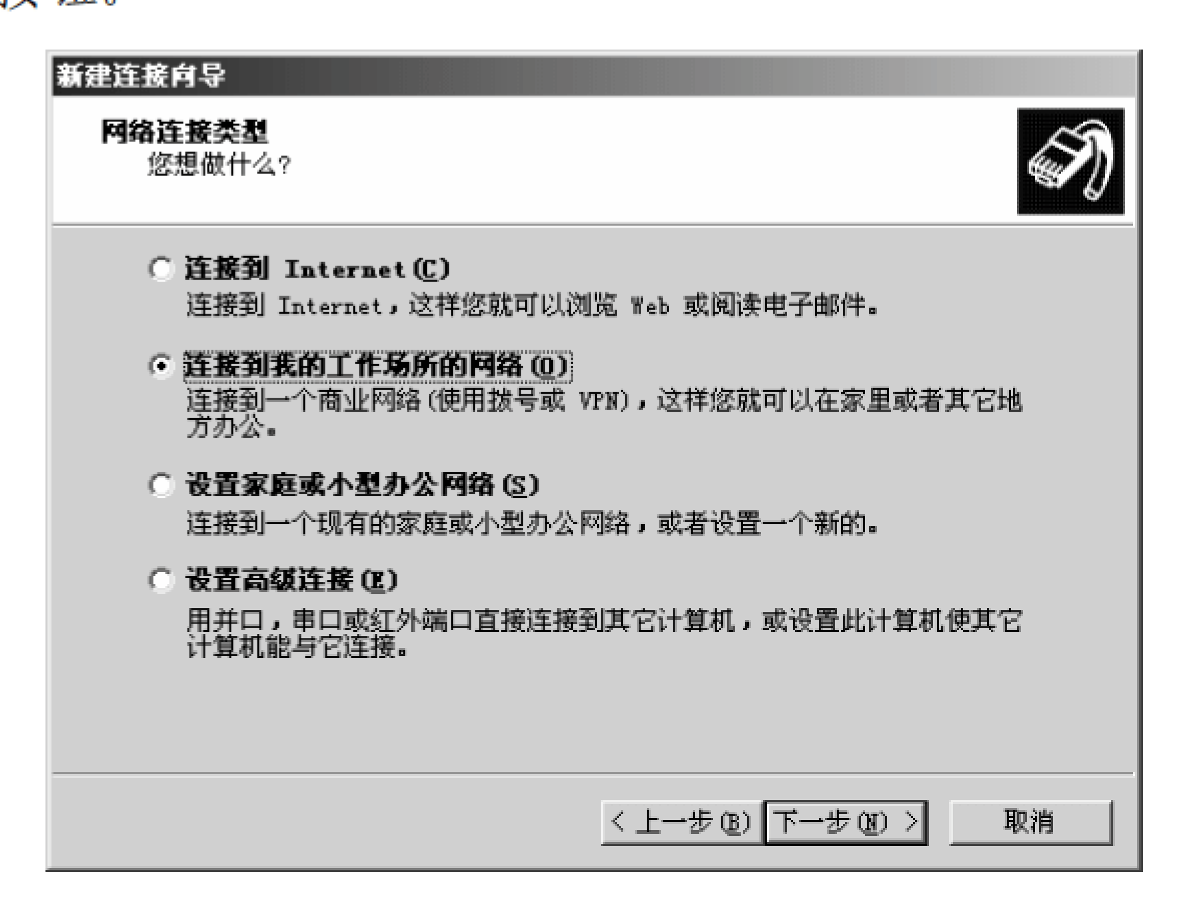


图 16-74

04 弹出【网络连接】对话框，选择【虚拟专用网络连接】单选按钮，如图 16-75 所示，单击【下一步】按钮。

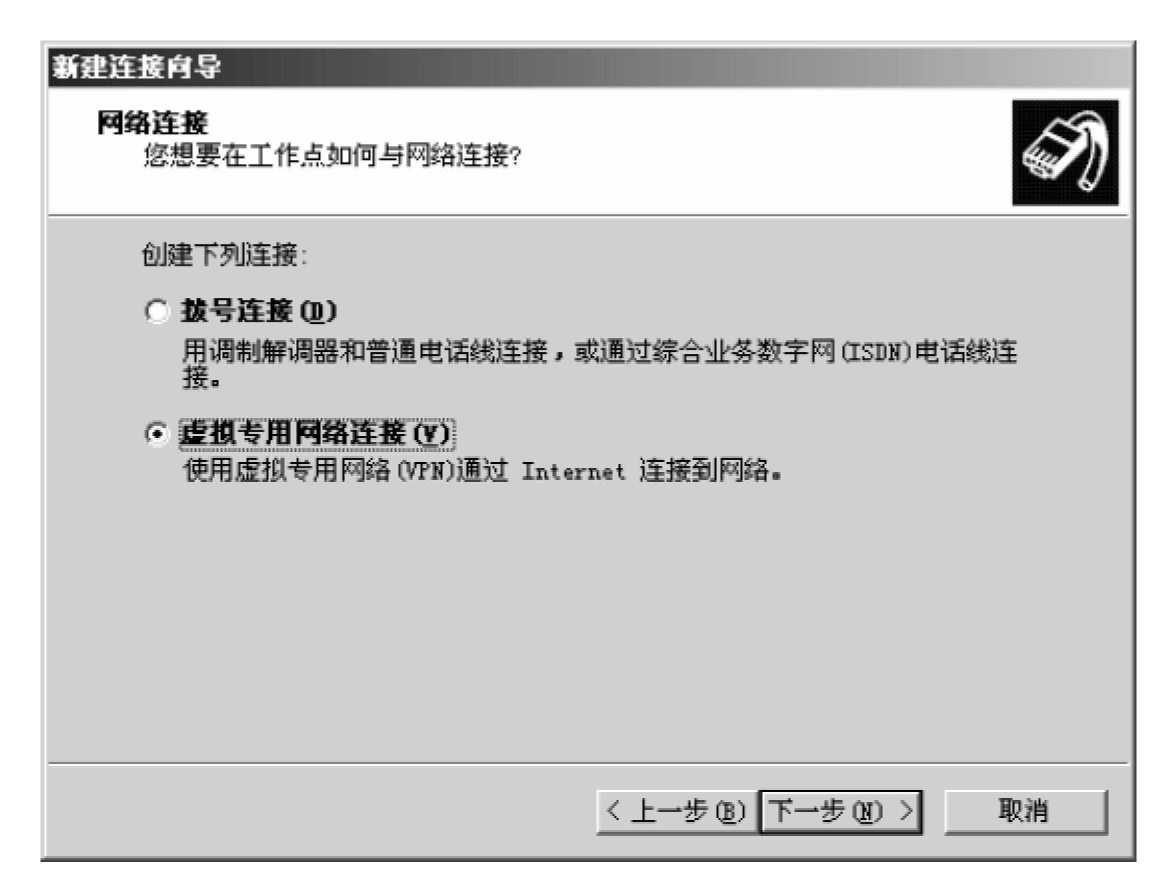


图 16-75

05 弹出【连接名】对话框，在【公司名】文本框中输入本次连接的名字“computerA”，为了方便记忆建议输入远程访问服务器所在公司名，单击【下一步】按钮，如图 16-76 所示。



图 16-76

06 弹出【VPN 服务器选择】对话框，如图 16-77 所示，在【主机名或 IP 地址】文本框输入远程访问服务器的地址，本实例为“61.192.93.100”，单击【下一步】按钮。



图 16-77

07 新建连接向导配置完成，为了方便连接，可以选择【在我的桌面上添加一个到此连接的快捷方式】单选按钮，如图 16-78 所示，单击【完成】按钮。

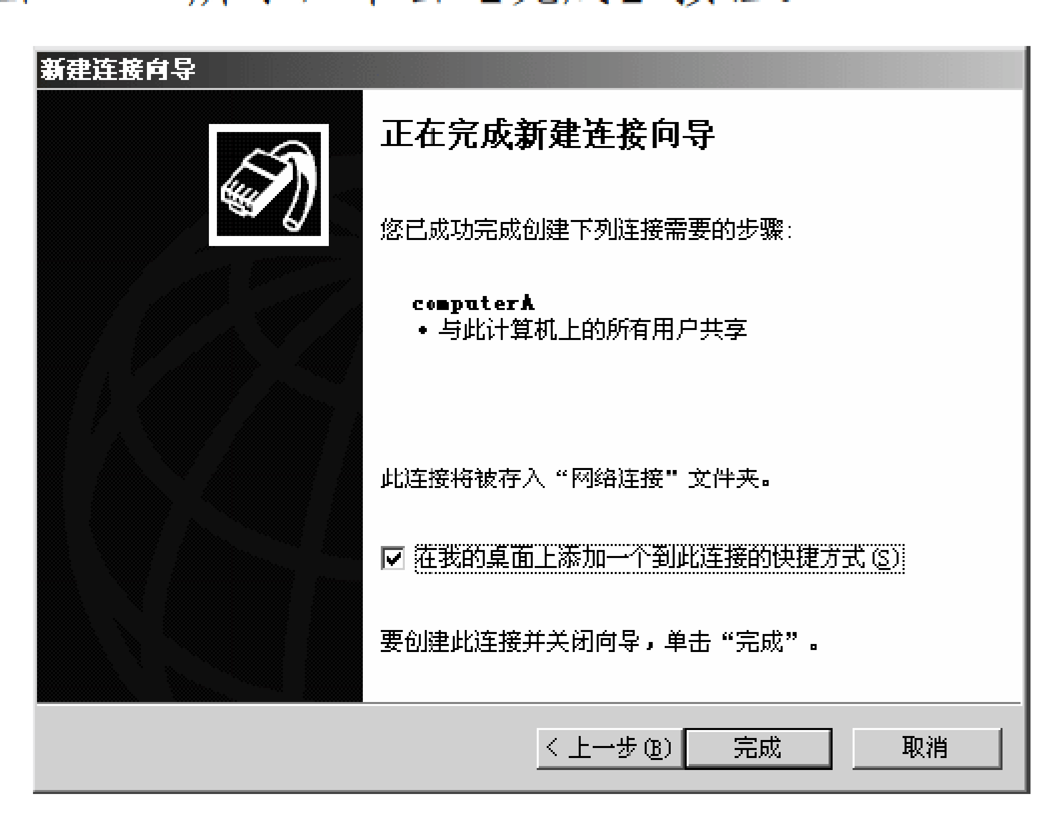


图 16-78

08 弹出【连接 computerA】对话框，在【用户名】和【密码】文本框输入进行身份认证的账户及密码信息，如图 16-79 所示，单击【连接】按钮。



图 16-79

09 自动认证连接，并从远程访问服务器获得 IP 地址，添加成功后会在【网络连接】窗口显示连接图标，如图 16-80 所示。



图 16-80

10 右击连接图标，选择【状态】菜单命令，弹出【computerA 状态】对话框，如图 16-81 所示，在【常规】选项卡中显示了连接状态，【活动】状态信息中的【压缩】状态表示信息使用 VPN 连接发送时的压缩比例，默认使用 VPN 传输的数据都进行了压缩。

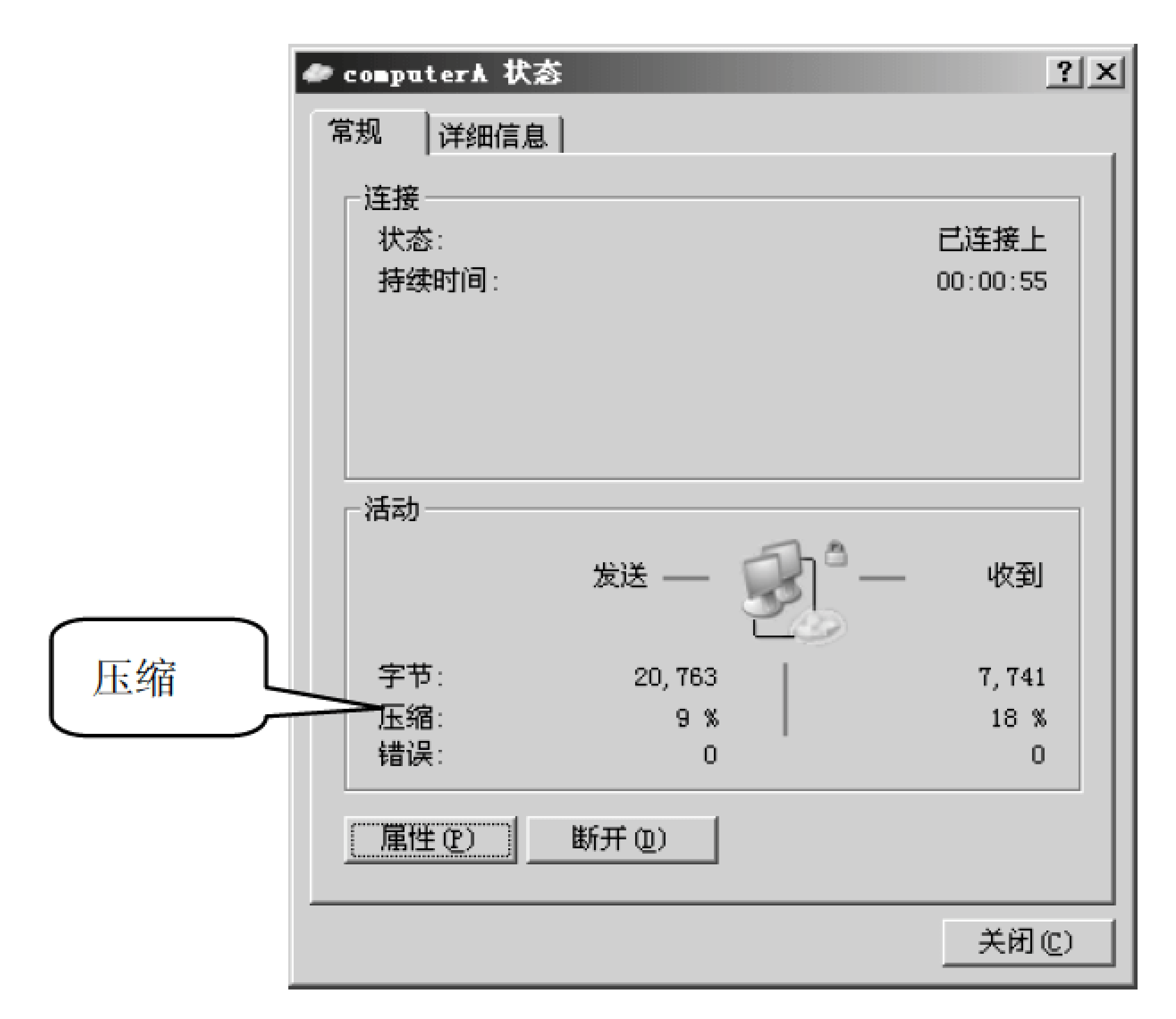


图 16-81

11 如图 16-82 所示，在【详细信息】选项卡中显示了客户端用于连接远程访问服务器的信息，包括：压缩方式、加密方式、身份验证方式、远程服务器地址、客户端地址等信息。



图 16-82

16.3.2 远程站点 VPN

远程站点 VPN 需要对两端分别配置，用户可以按照如图 16-83 所示的拓扑图实现方案配置，具体的配置步骤如下。

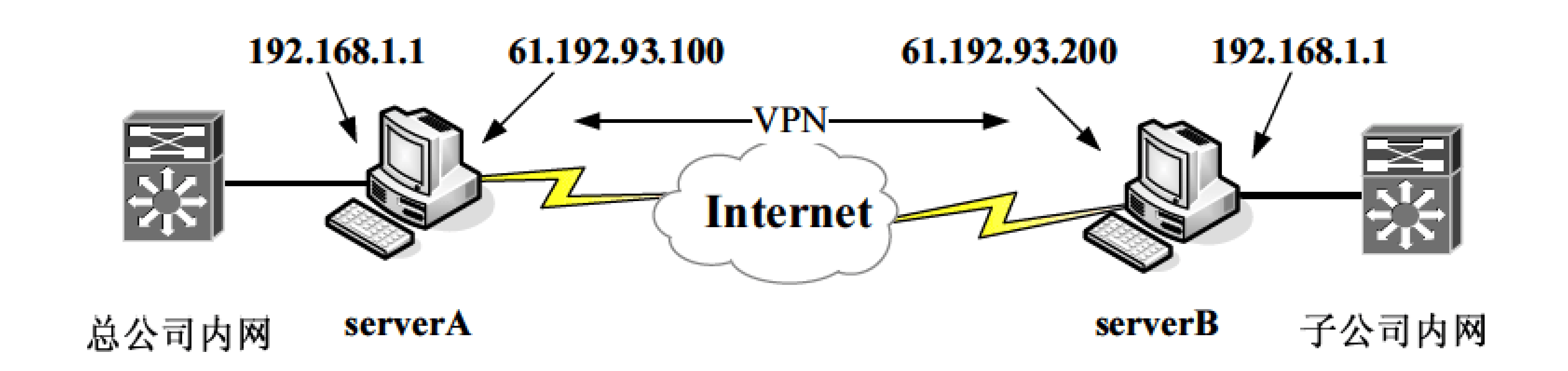


图 16-83

1. serverA ISA 服务器的配置

具体的操作步骤如下。

01 打开 ISA Server 2006 程序主界面，在左侧选项列表中选择【虚拟专用网（VPN）】选项，选择【远程站点】选项卡，选择右侧【任务】选项卡的【创建 VPN 点对点连接】选项，如图 16-84 所示。

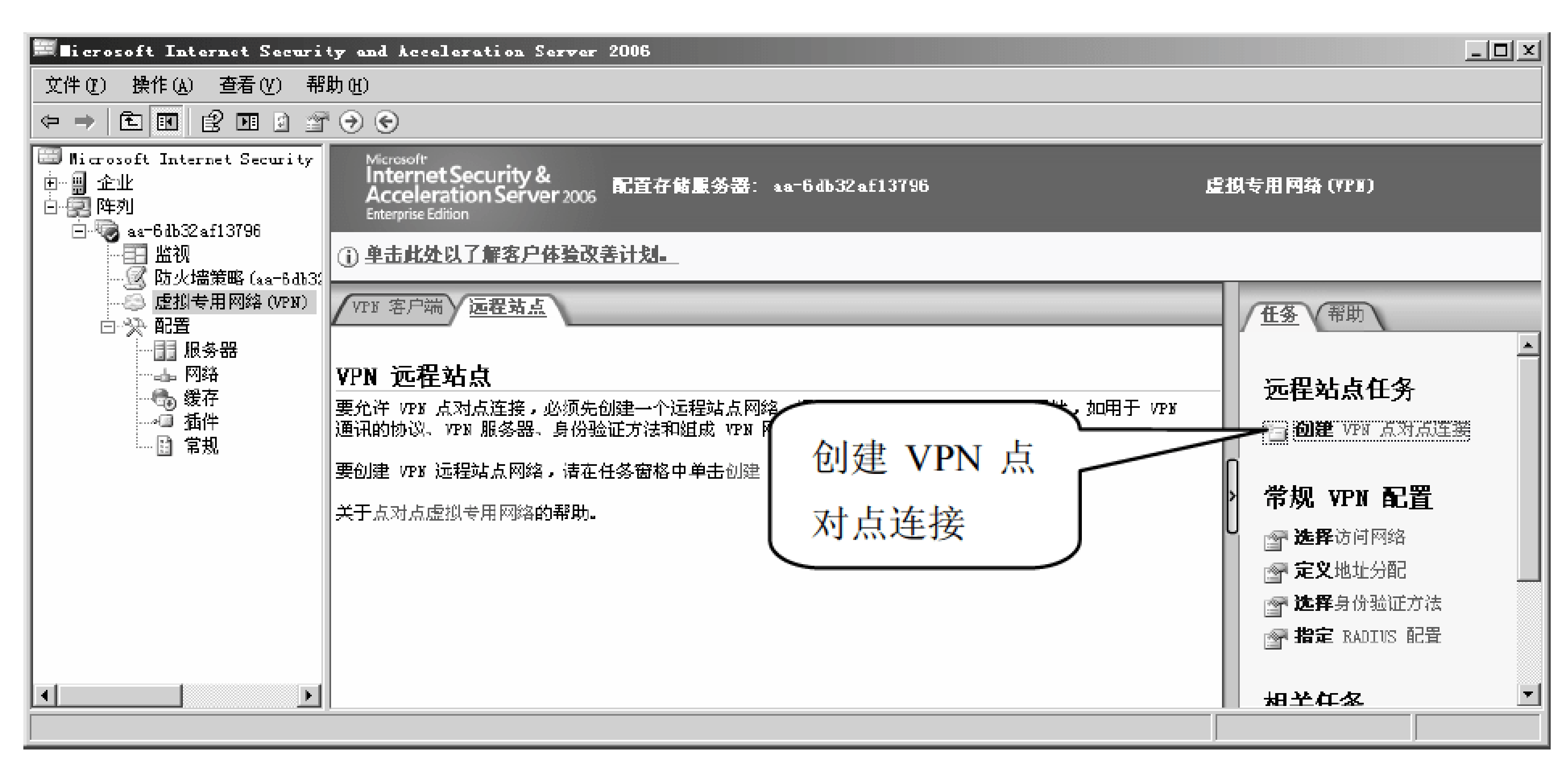


图 16-84

02 弹出【创建点对点连接向导】对话框，在【点对点网络名称】文本框中输入“serverA”，单击【下一步】按钮，如图 16-85 所示。

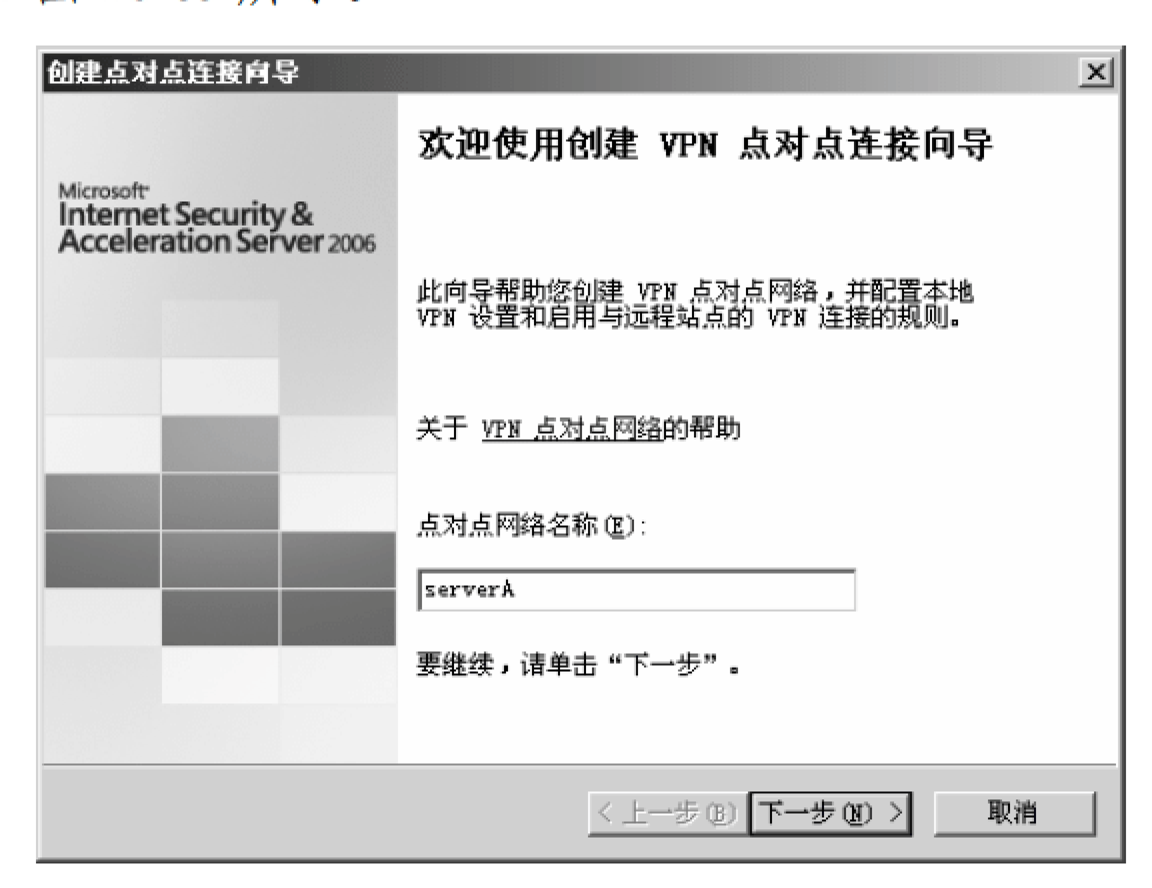


图 16-85

03 弹出【VPN 协议】对话框，现在本连接使用的隧道协议，选择【IPsec 上的第二层隧道协议（L2TP）】单选按钮，如图 16-86 所示，单击【下一步】按钮。

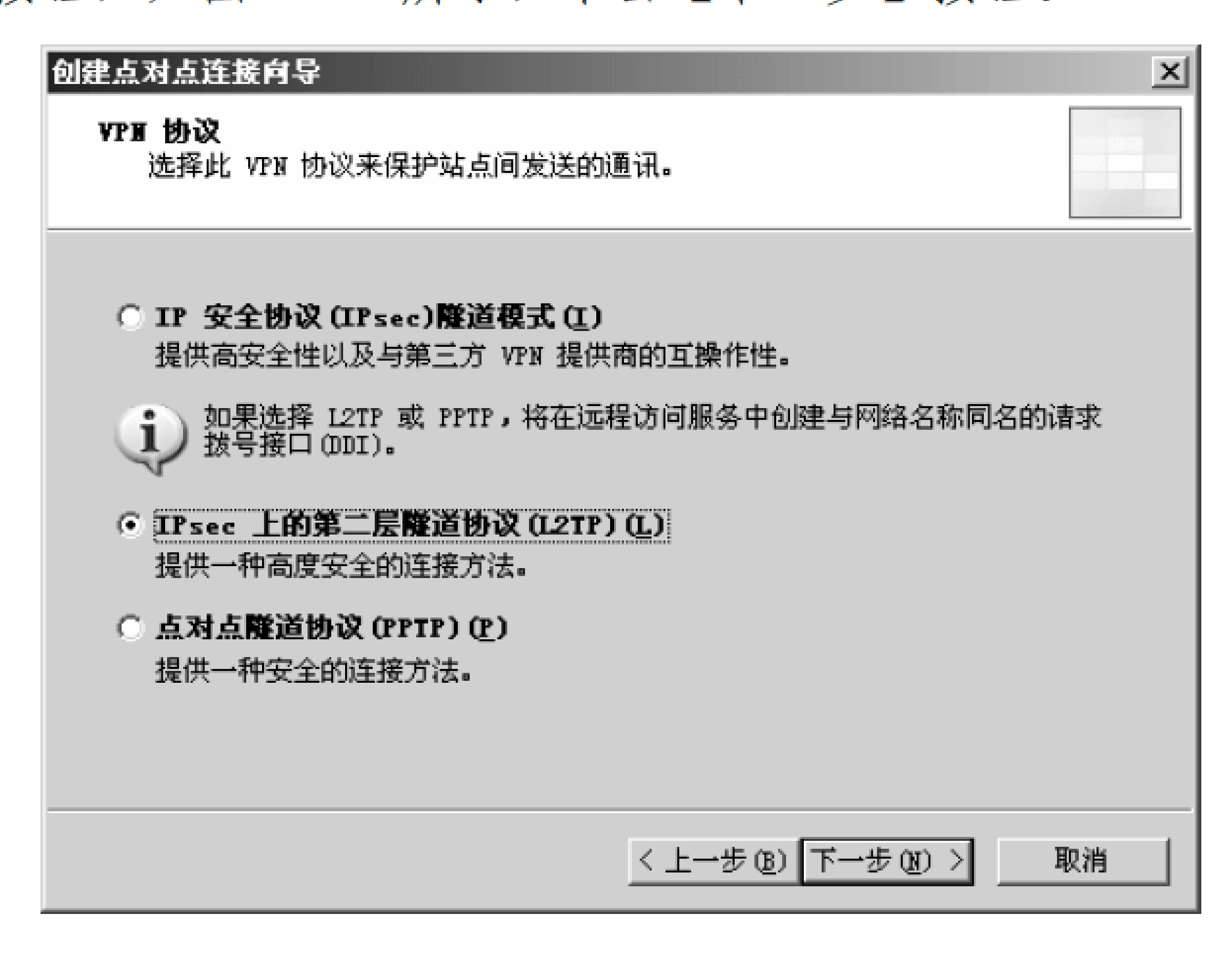


图 16-86

04 弹出提示框，如图 16-87 所示，提示远程站点连接本站点进行身份认证的账户必须和本向导创建的网络同名，即本向导创建了“serverA”，那么对端站点必须要创建“serverA”账户，并配置拨入访问权限，单击【确定】按钮。



图 16-87

05 弹出【连接所有者】对话框，选择默认配置，单击【下一步】按钮，如图 16-88 所示。

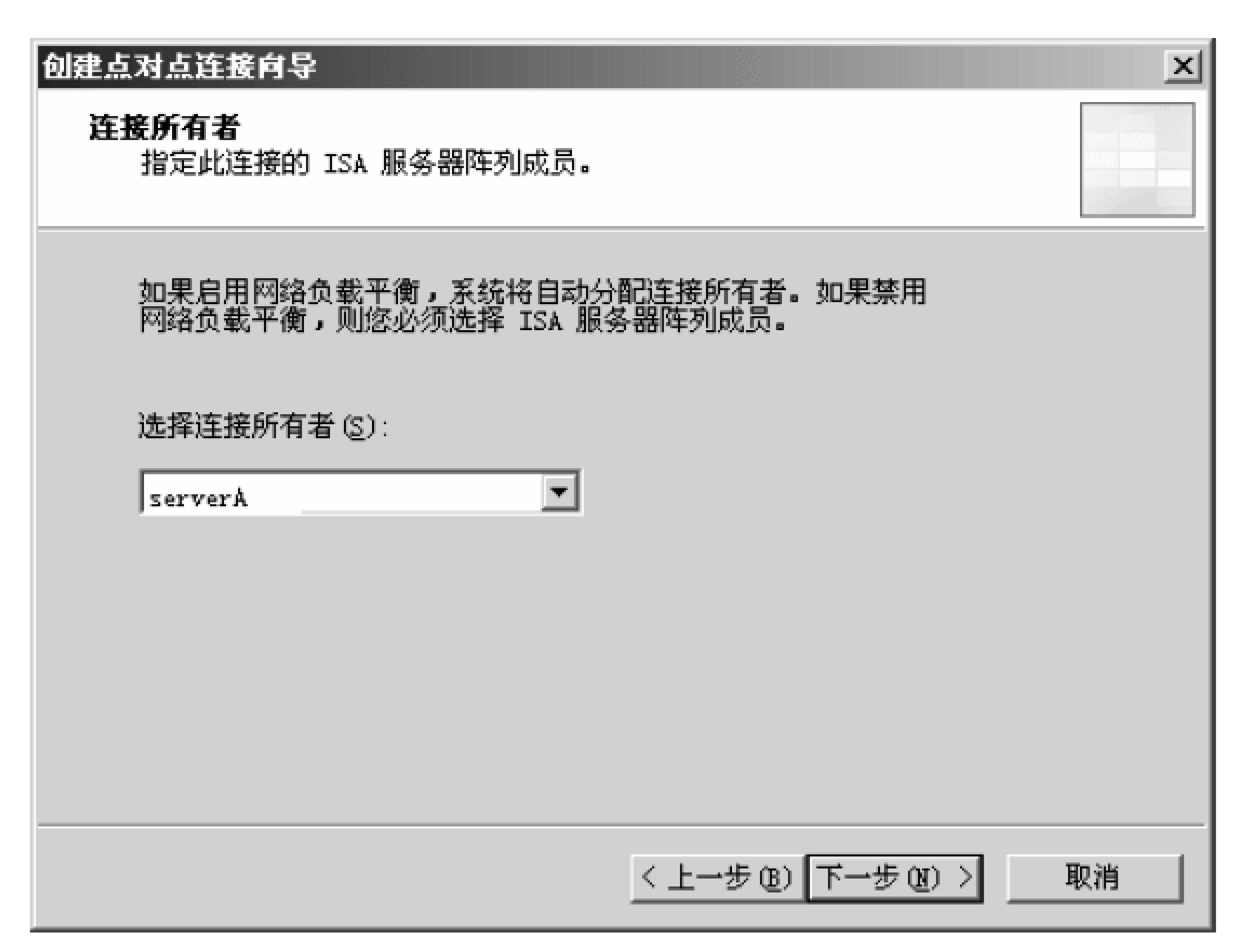


图 16-88

06 弹出【远程站点网关】对话框，如图 16-89 所示，在【远程站点 VPN 服务器】文本框中

输入远程站点的 IP 地址“61.192.93.200”，单击【下一步】按钮。

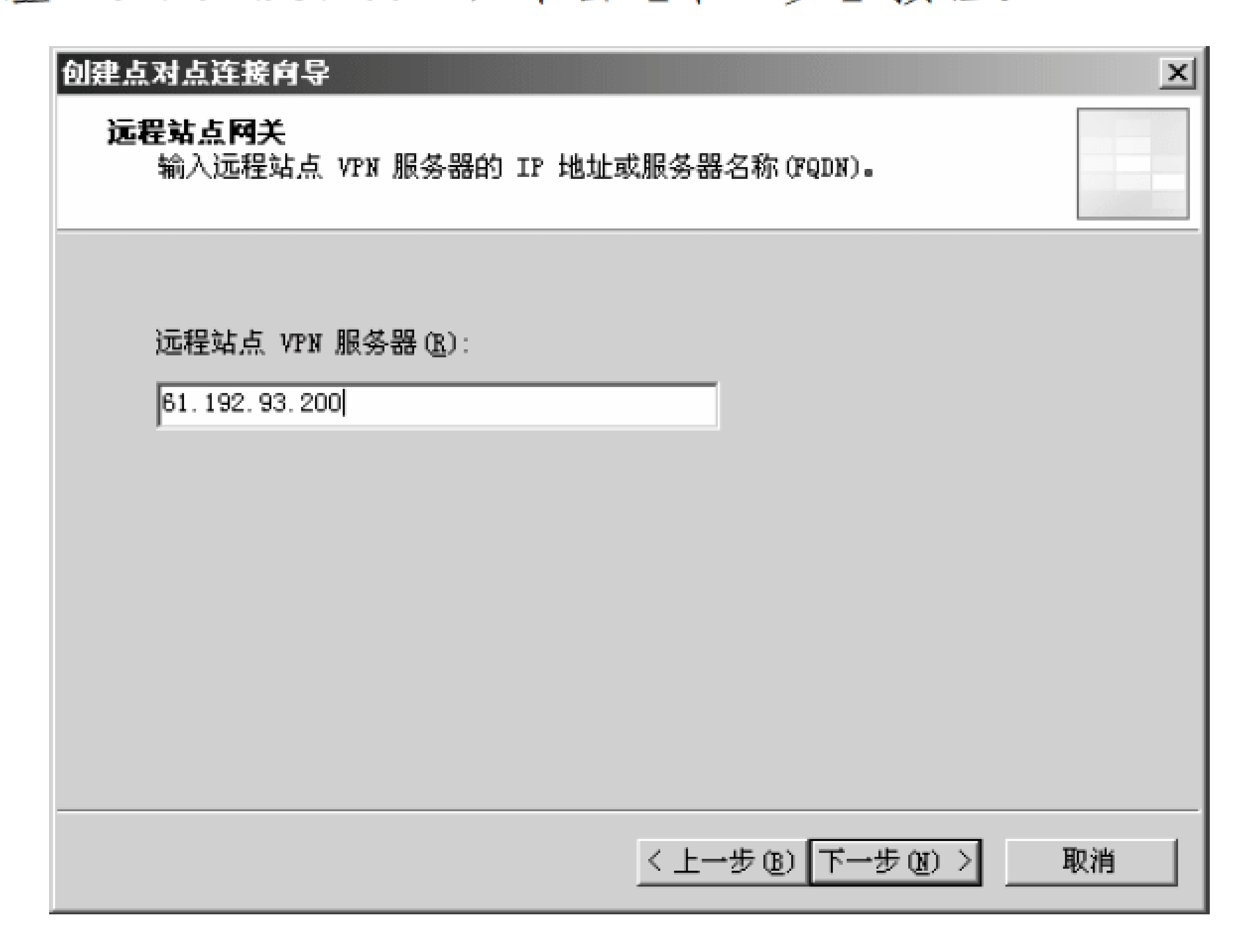


图 16-89

07 弹出【远程身份验证】对话框，如图 16-90 所示，配置允许本地站点连接远程站点的账户信息，用户名必须是远程站点创建的 VPN 点对点连接的网络名，本实例采用“serverB”，单击【下一步】按钮。

创建点对点连接向导
远程身份验证
为了使本地站点能够启动到远程站点的连接，需要远程站点上的用户帐户进行身份验证。
允许本地站点使用此用户帐户启动到远程站点的连接(A):
此用户帐户必须与在远程站点上创建的 VPN 点对点连接的名称匹配。
用户名(U): serverB
域(D):
密码(P): ******
确认密码(C): ******
< 上一步(B) 下一步(N) > 取消

图 16-90

08 弹出【L2TP/IPsec 传出身份验证】对话框，如图 16-91 所示，如果站点两端都可以从同一个证书认证机构获得数字证书则选择【证书身份验证】单选按钮，本实例采用【预共享密钥身份验证】，预共享密钥为“serverAB”，单击【下一步】按钮。

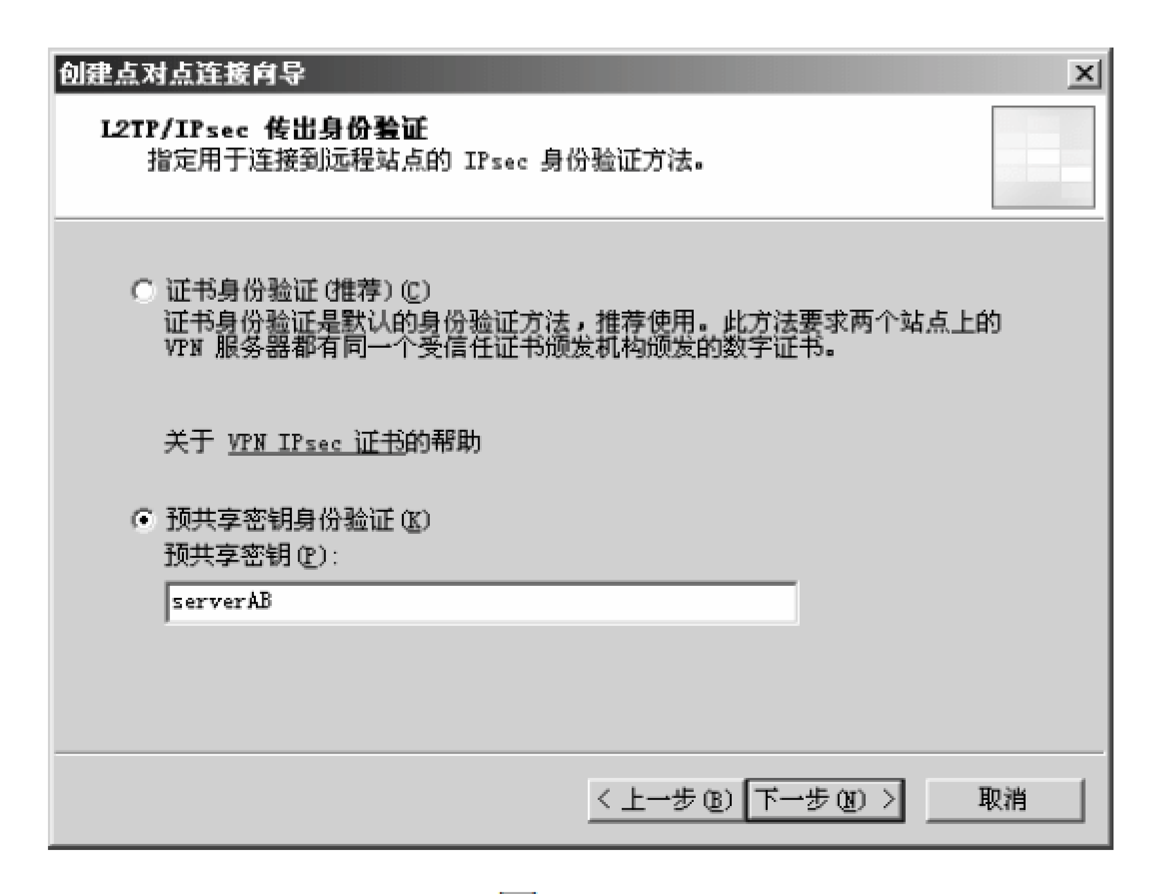


图 16-91

09 弹出【输入 L2TP/IPsec 身份验证】对话框，如图 16-92 所示，在【预共享密钥】文本框中输入“serverAB”，单击【下一步】按钮。

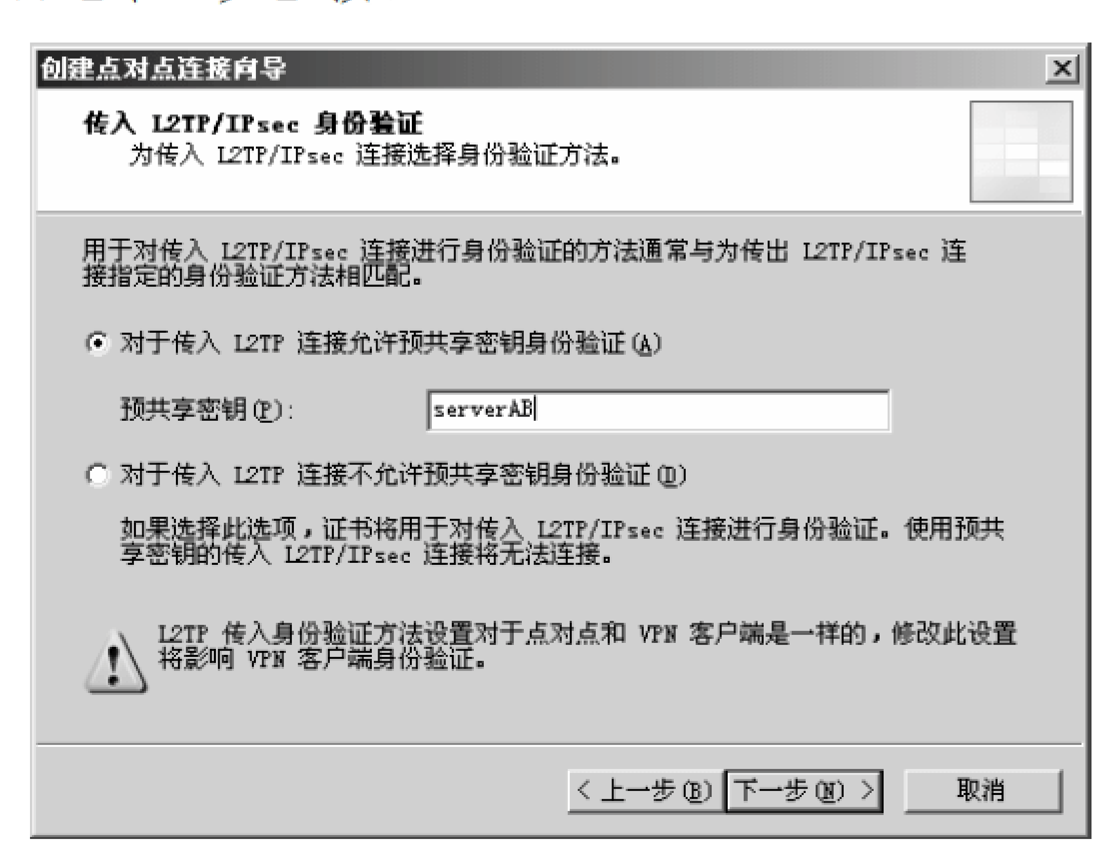


图 16-92

10 弹出【网络地址】对话框，如图 16-93 所示，单击【添加范围】按钮，设置远程站点使用的内部私有地址范围。



图 16-93

11 弹出【IP 地址范围属性】对话框，如图 16-94 所示，在【起始地址】和【结束地址】文本框中输入地址范围“192.168.1.0~192.168.1.255”，单击【确定】按钮。



图 16-94

12 返回【网络地址】对话框，【地址范围】选项列表中已经显示添加的地址范围，如图 16-95 所示，单击【下一步】按钮。

图 16-95

13 弹出【远程 NLB】对话框，如图 16-96 所示，如果使用了负载平衡技术可以使用该配置，本实例不使用，单击【下一步】按钮。

图 16-96

14 弹出【点对点网络规则】对话框，采用默认配置，单击【下一步】按钮，如图 16-97 所示。

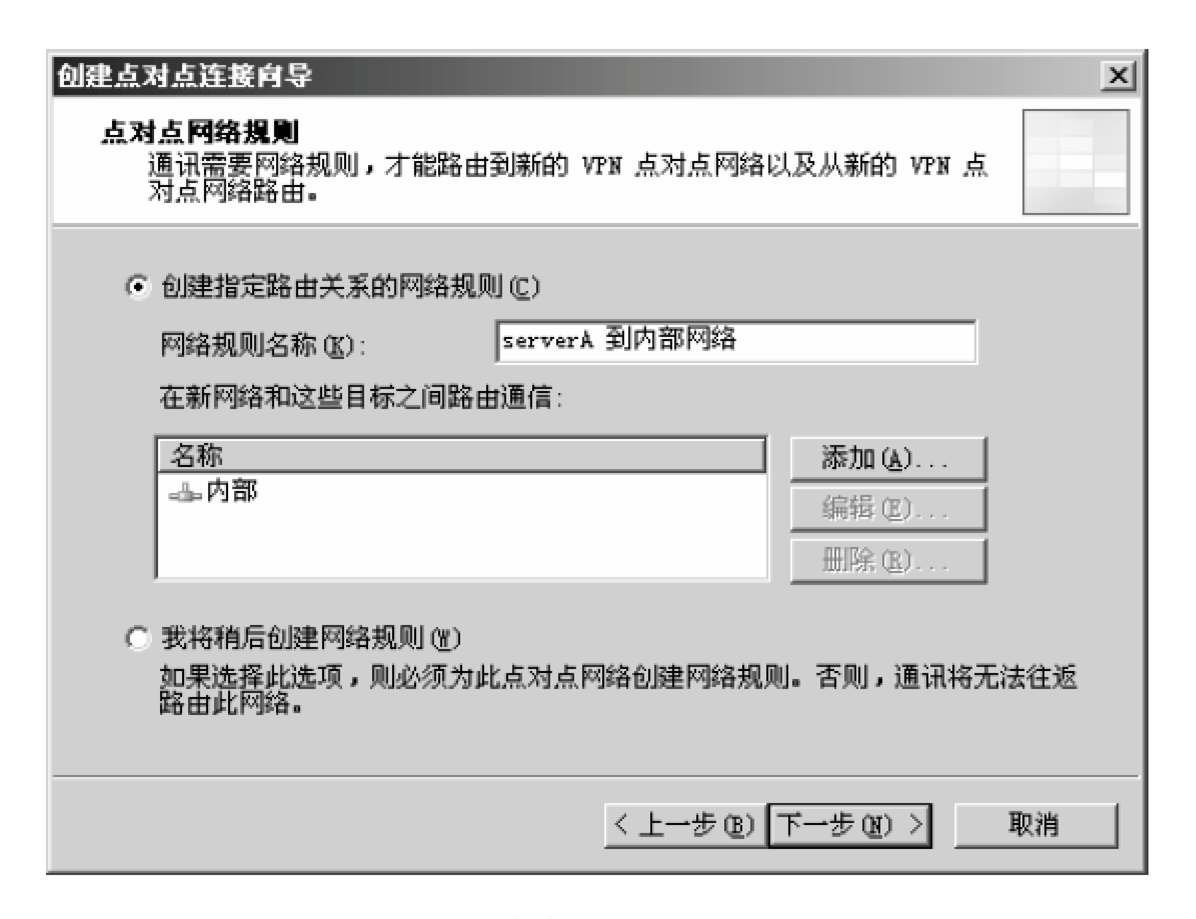


图 16-97

15 弹出【点对点网络访问规则】对话框，如图 16-98 所示，在【将规则应用于这些协议】下拉菜单选项中选择【所有出站通信】选项，单击【下一步】按钮。

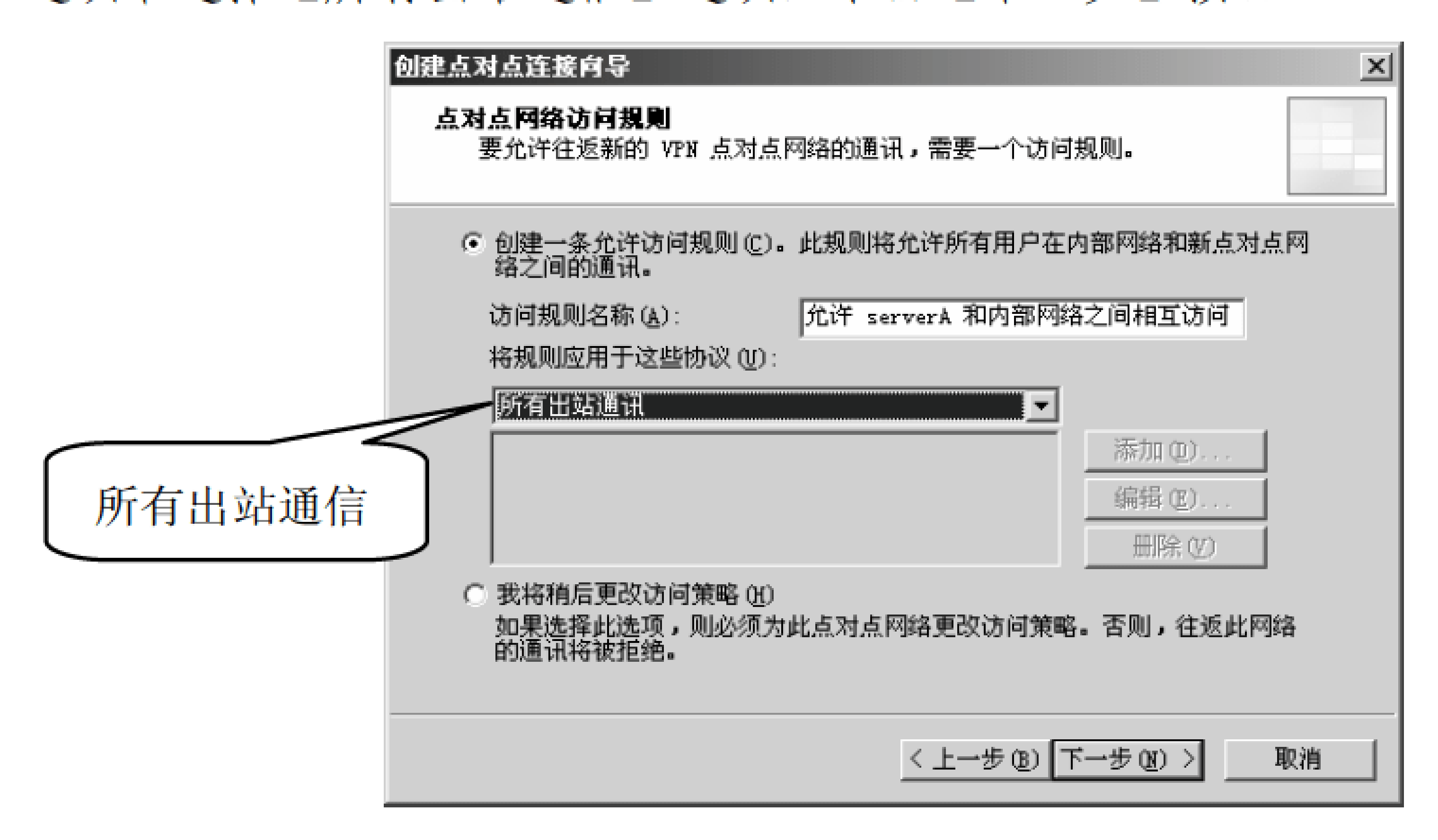


图 16-98

16 VPN 点对点连接配置完成，显示出配置信息，单击【完成】按钮，结束向导，如图 16-99 所示。

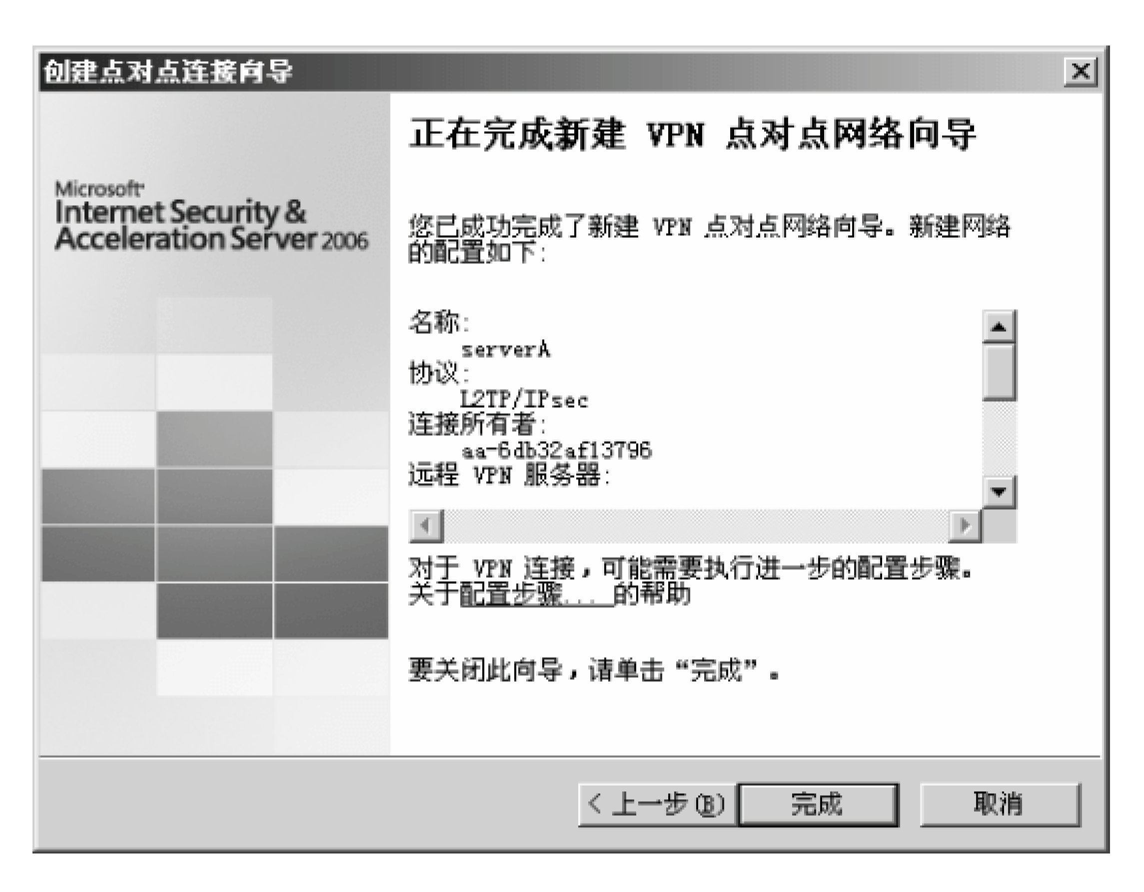


图 16-99

17 弹出【ISA Server 2006】提示框，远程访问服务重启，单击【确定】按钮，如图 16-100 所示。

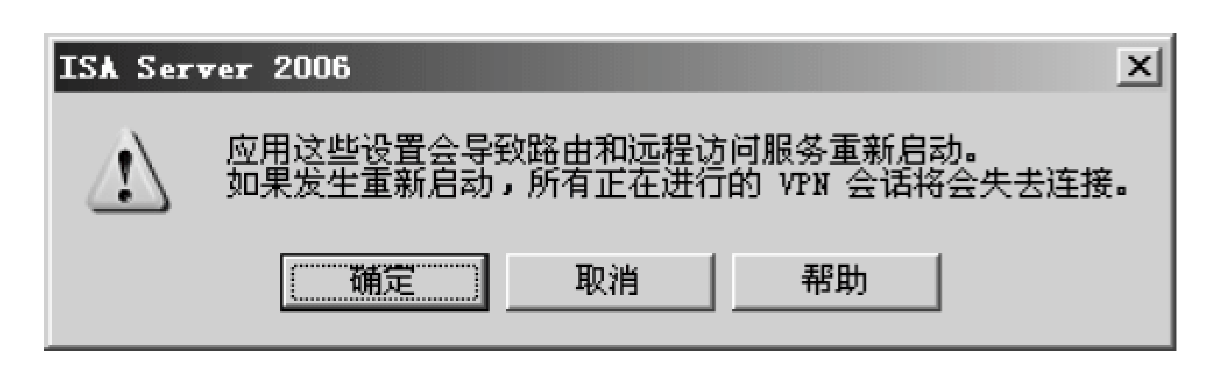


图 16-100

18 弹出【剩余 VPN 点对点任务】提示框，如图 16-101 所示，提示还有哪些 VPN 连接配置没有完成，可按照给出的提示继续配置点对点的 VPN 连接，单击【确定】按钮。



图 16-101

19 弹回程序主界面，如图 16-102 所示，在【远程站点】选项卡下显示出新增加的 VPN 连接状态信息，单击【应用】按钮，使配置生效。



图 16-102

20 如图 16-103 所示，在左侧列表中选择【防火墙策略】选项，在右侧【防火墙策略规则】列表中显示了新增的 VPN 流量通信规则。

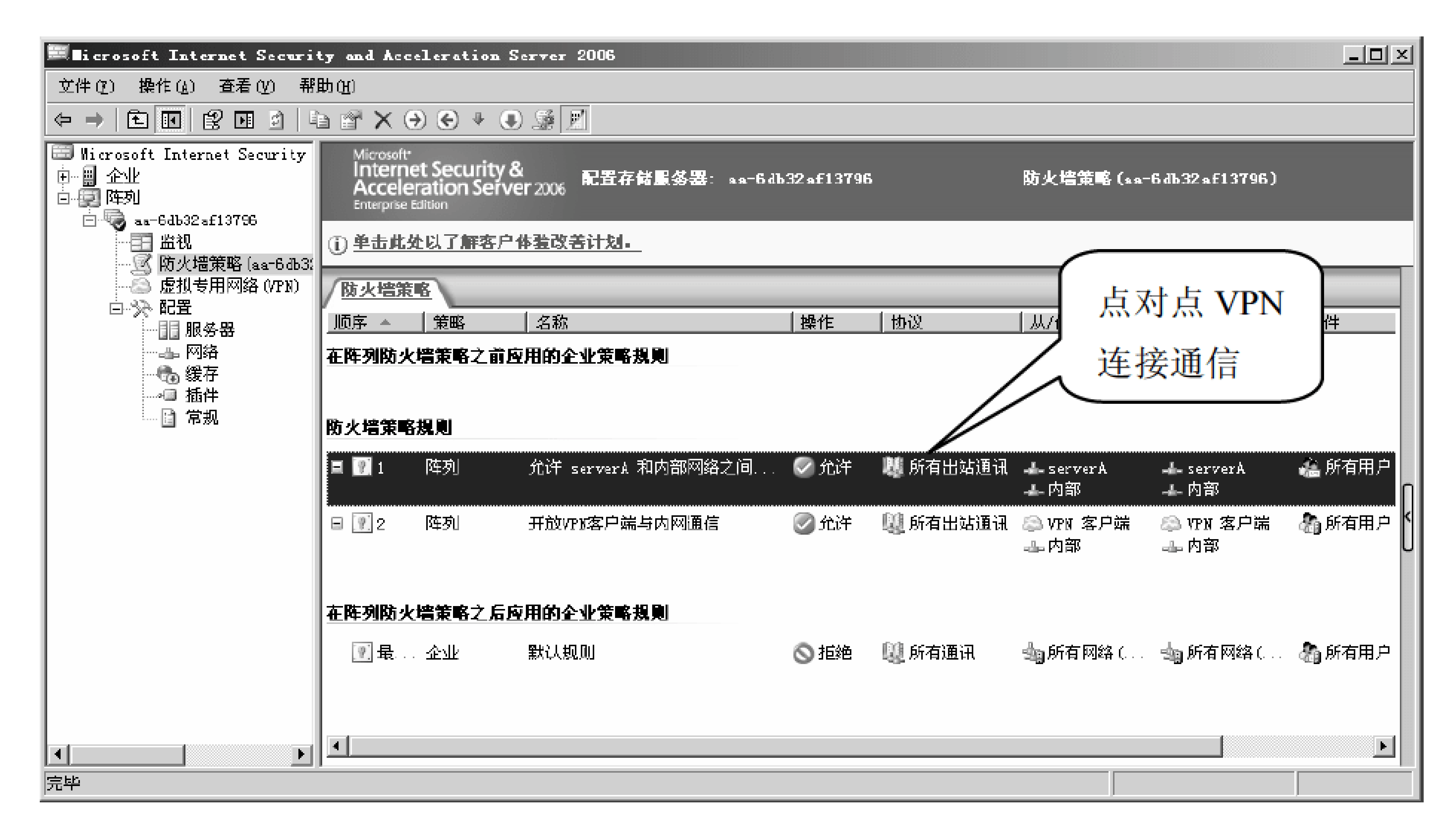


图 16-103

21 在桌面右击【我的电脑】图标，在弹出的快捷菜单中选择【管理】菜单命令，如图 16-104 所示。



图 16-104

22 弹出【计算机管理】窗口，如图 16-105 所示，在左侧选项列表中选择【计算机管理】➢【系统工具】➢【本地用户和组】➢【用户】选项，右击【用户】选项，选择【新用户】菜单命令。



图 16-105

23 弹出【新用户】对话框，如图 16-106 所示，在【用户名】文本框中输入“serverB”，选择【用户不能更改密码】和【密码永不过期】复选框，单击【创建】按钮。



图 16-106

24 右击 serverB 账户，在弹出的快捷菜单中选择【属性】菜单命令，如图 16-107 所示。



图 16-107

25 弹出【serverB 属性】对话框，如图 16-108 所示，选择【拨入】选项卡，在【远程访问权限】中有三个选项，如果不使用远程访问策略，直接选【允许访问】单选按钮，单击【确定】按钮。

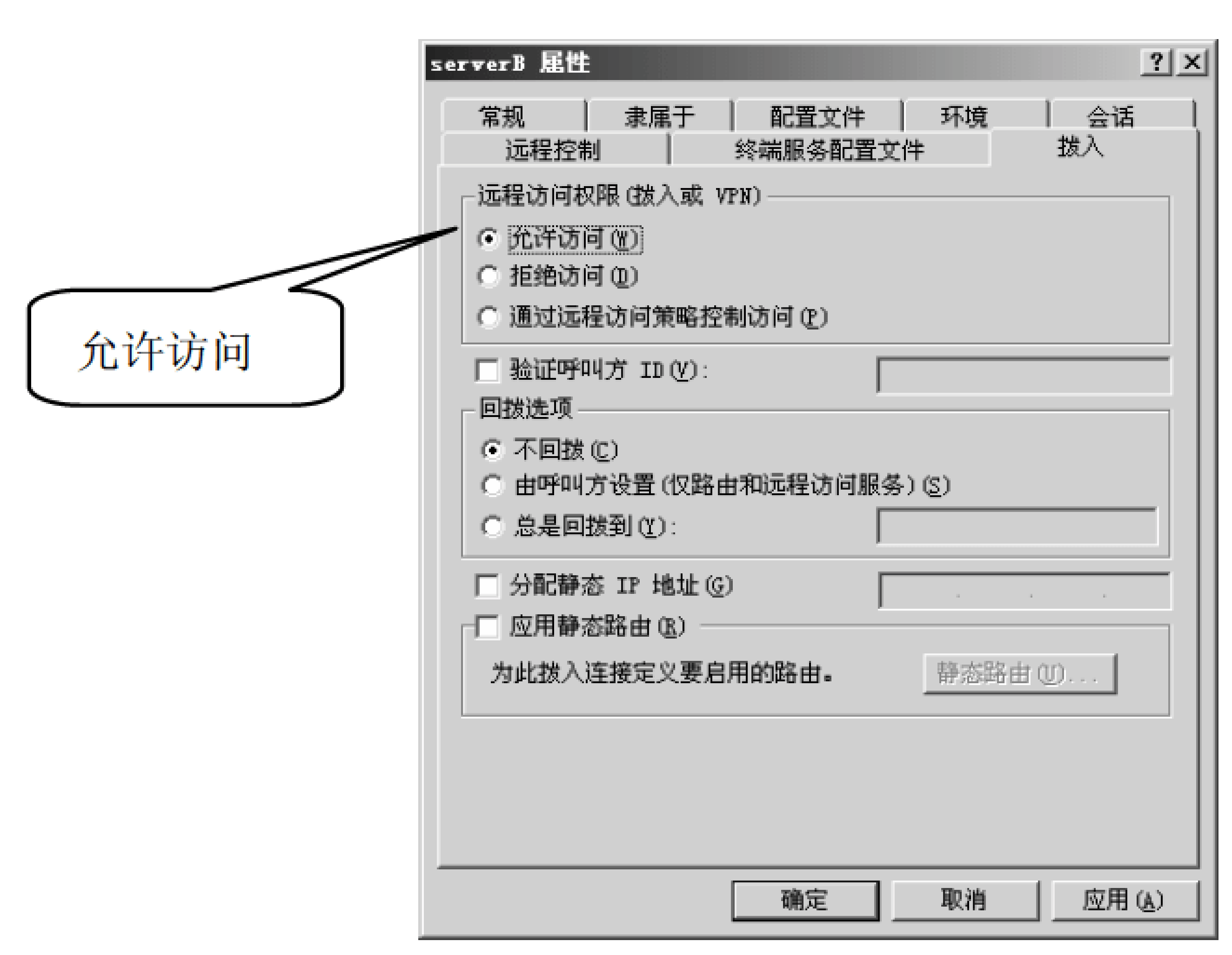


图 16-108

2. serverB ISA 服务器的配置

具体的操作步骤如下。

01 打开 ISA Server 2006 程序主界面，如图 16-109 所示，在左侧选项列表中选择【虚拟专用网（VPN）】选项，选择【远程站点】选项卡，选择右侧【任务】选项卡的【创建 VPN 点对点连接】选项。

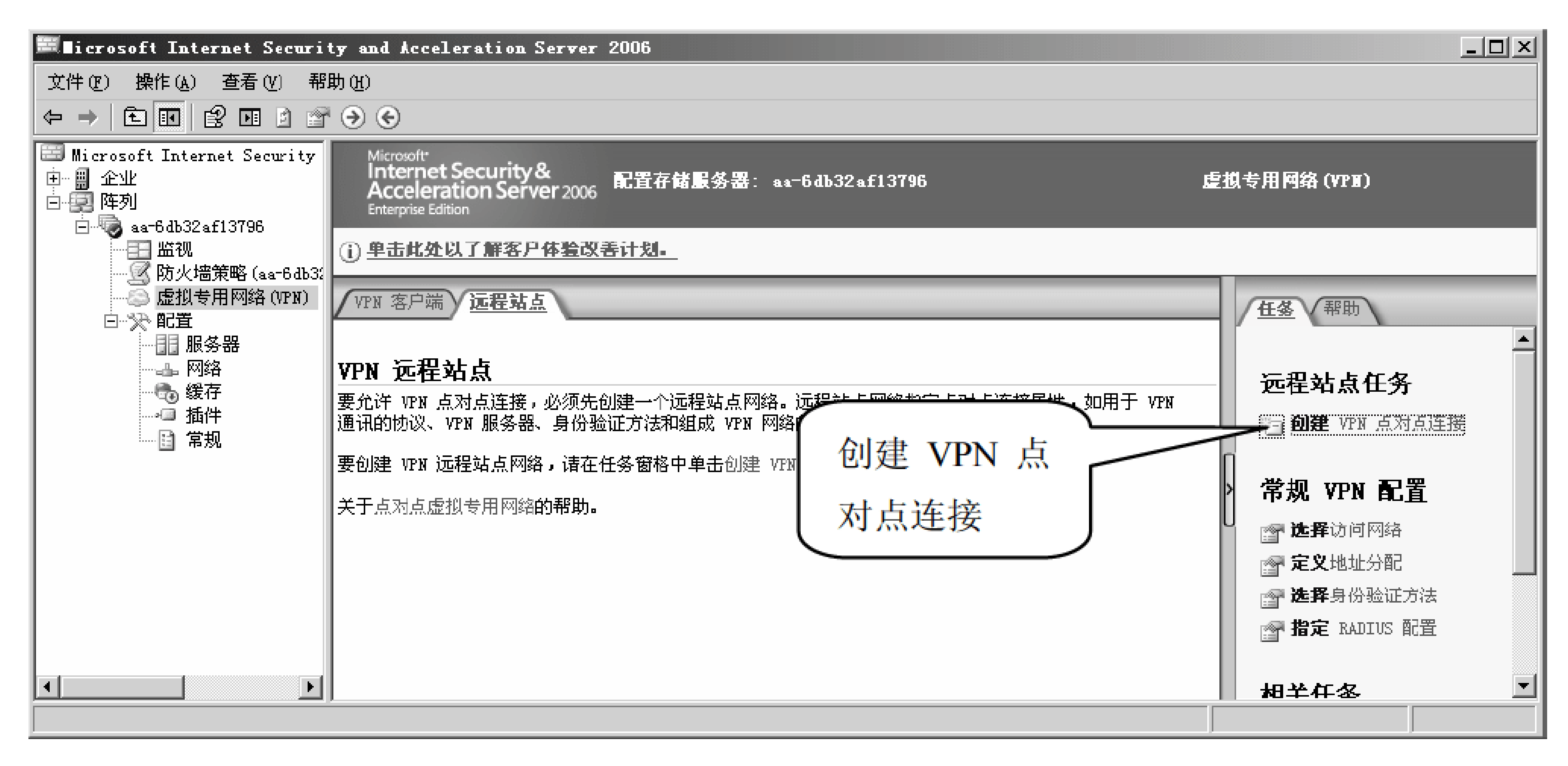


图 16-109

02 弹出【创建点对点连接向导】对话框，如图 16-110 所示，在【点对点网络名称】文本框中输入“serverB”，单击【下一步】按钮。

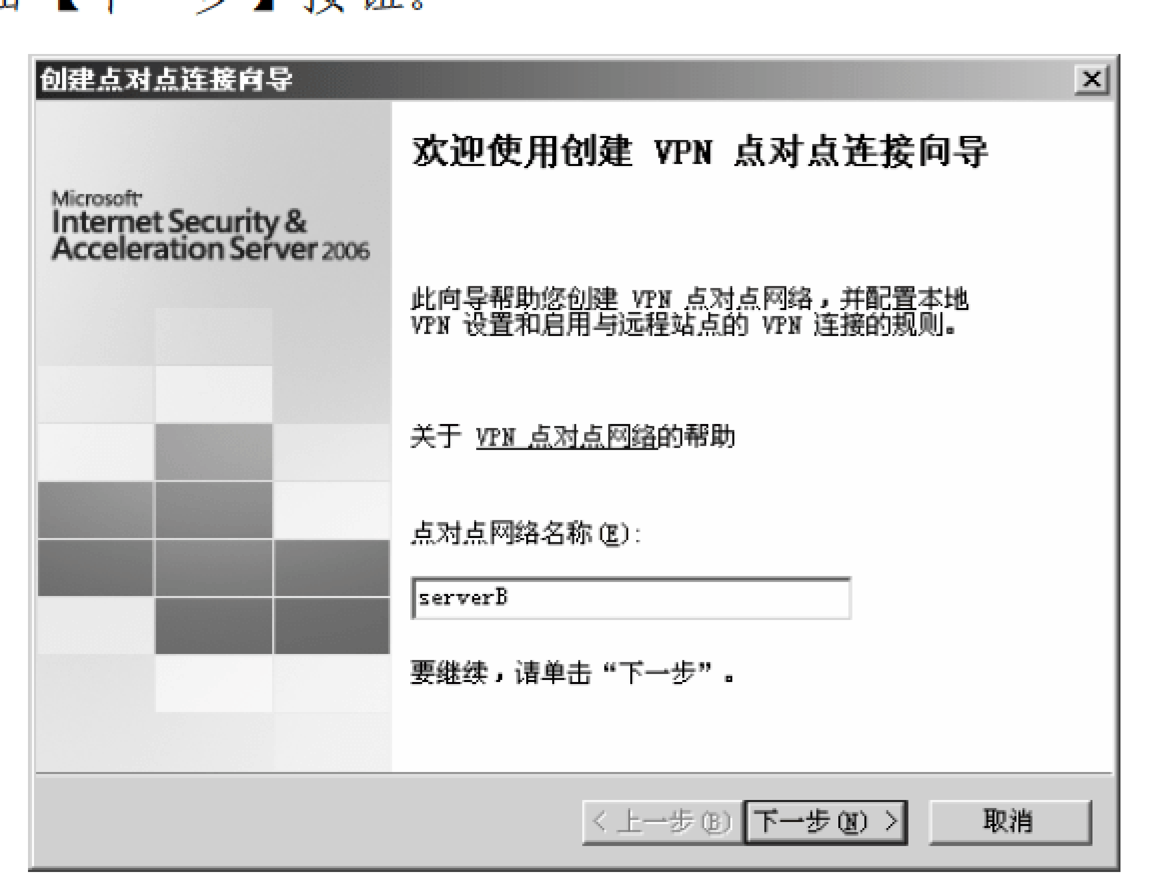


图 16-110

03 弹出【VPN 协议】对话框，如图 16-111 所示，现在本连接使用的隧道协议，选择【IPsec 上的第二层隧道协议（L2TP）】单选按钮，单击【下一步】按钮。

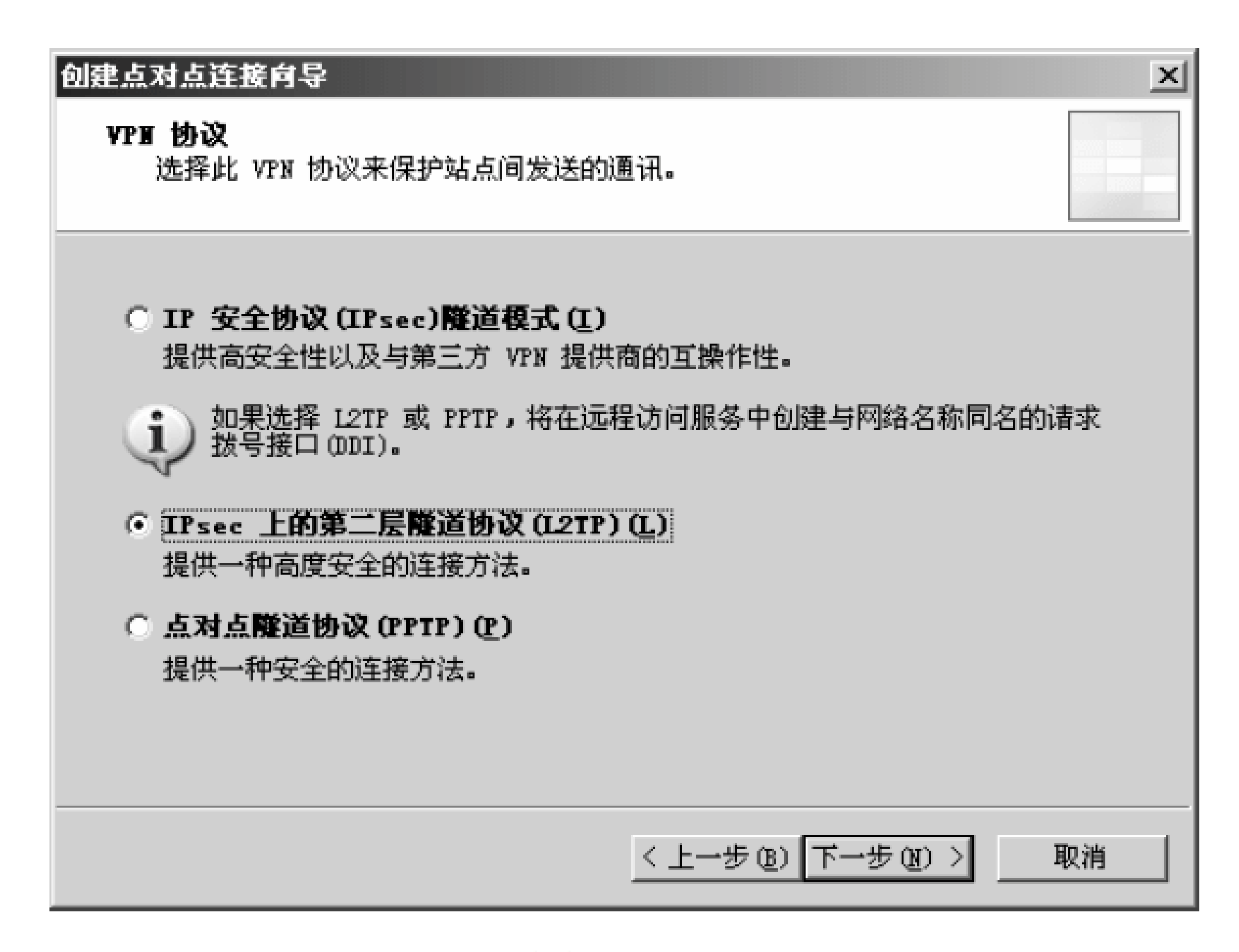


图 16-111

04 弹出提示框，如图 16-112 所示，提示远程站点连接本站点进行身份认证的账户必须和本向导创建的网络同名，即本向导创建了“serverB”，那么对端站点必须要创建“serverB”账户，并配置拨入访问权限，单击【确定】按钮。



图 16-112

05 弹出【连接所有者】对话框，如图 16-113 所示，选择默认配置，单击【下一步】按钮。

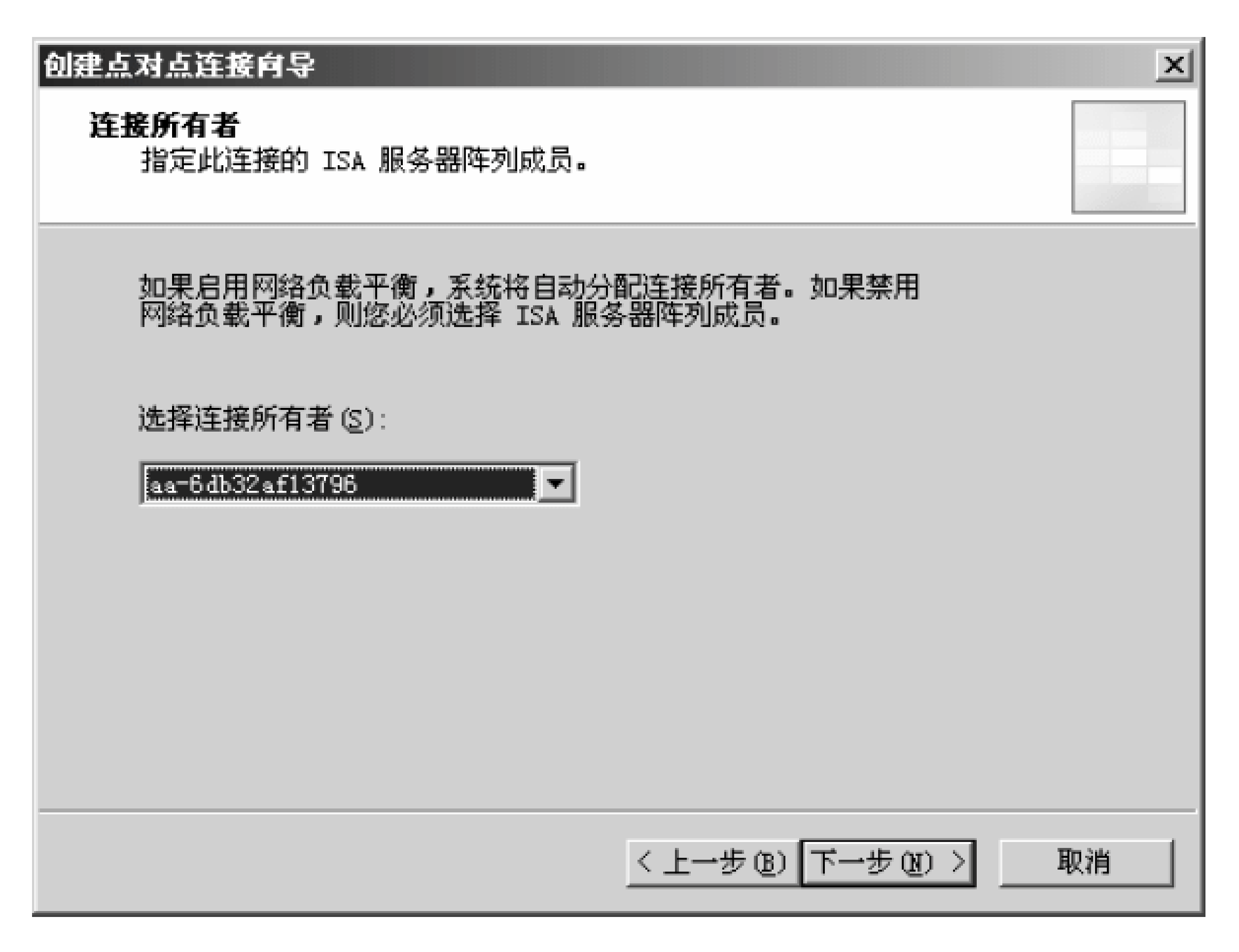


图 16-113

06 弹出【远程站点网关】对话框，如图 16-114 所示，在【远程站点 VPN 服务器】文本框中输入远程站点的 IP 地址“61.192.93.100”，单击【下一步】按钮。

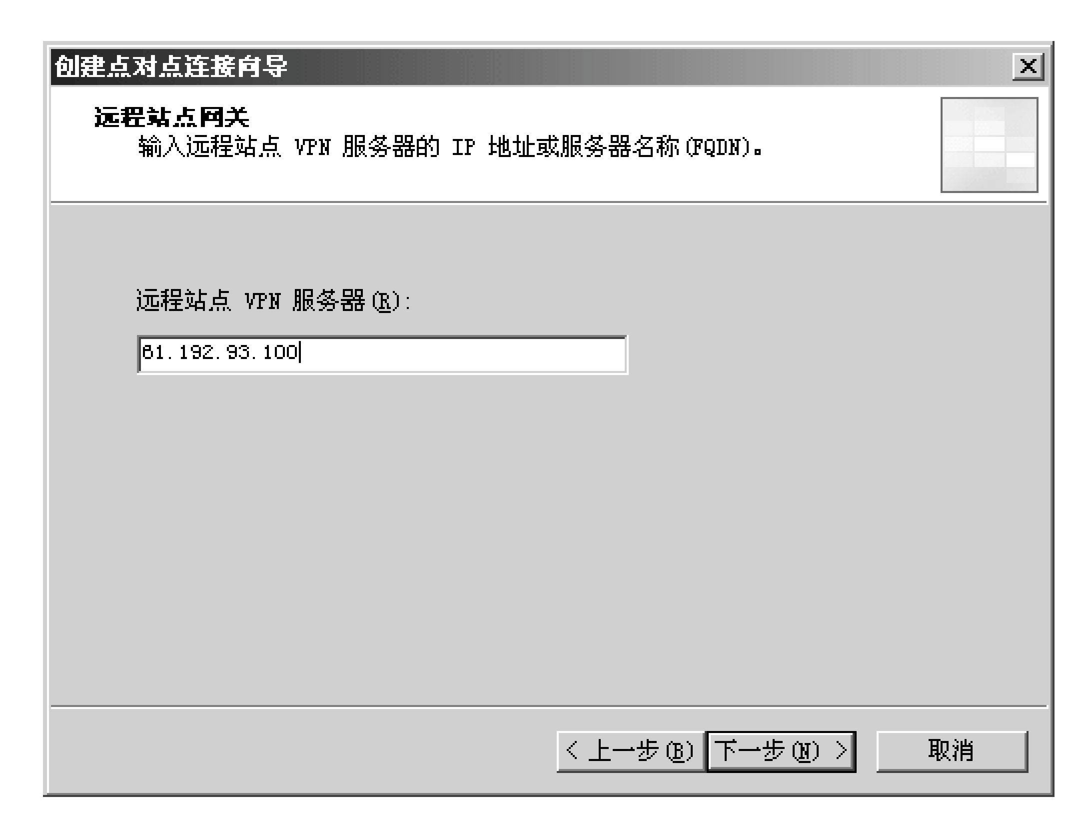


图 16-114

07 弹出【远程身份验证】对话框，如图 16-115 所示，配置允许本地站点连接远程站点的账户信息，用户名必须是远程站点创建的 VPN 点对点连接的网络名，本实例采用“serverA”，单击【下一步】按钮。

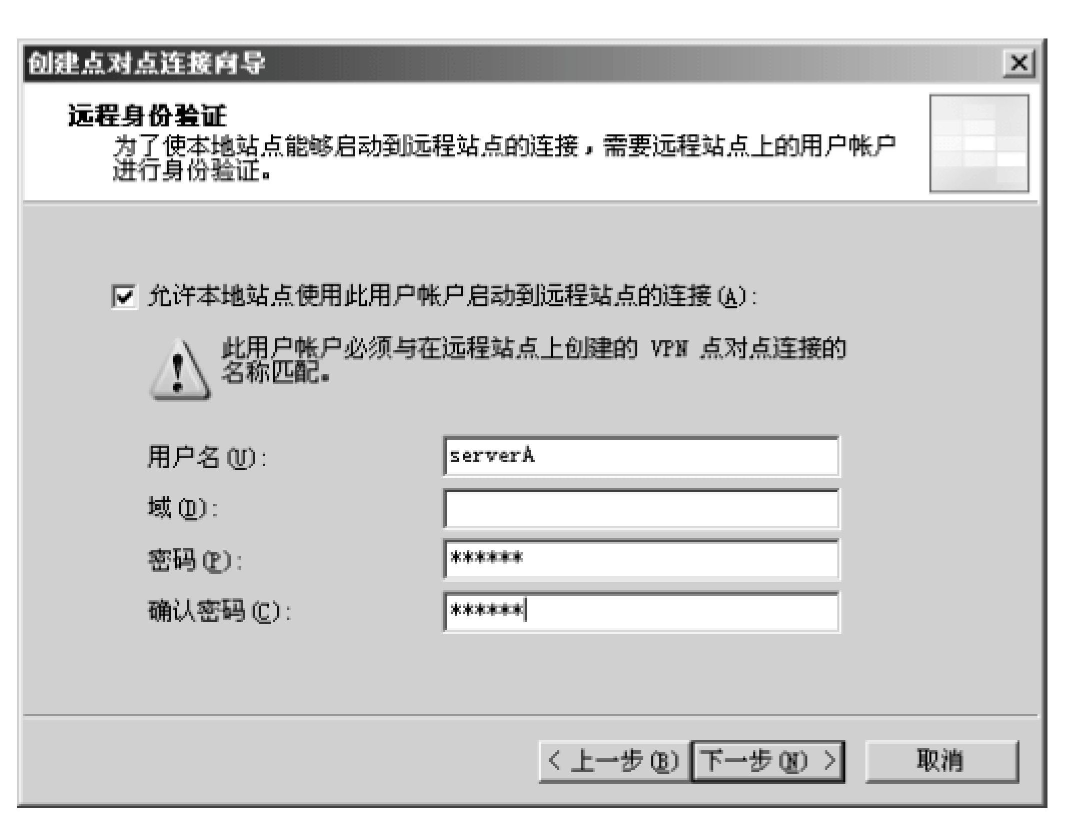


图 16-115

08 弹出【L2TP/IPsec 传出身份验证】对话框，如图 16-116 所示，如果站点两端都可以从同一个证书认证机构获得数字证书，则选择【证书身份验证】单选按钮，本实例采用【预共享密钥身份验证】，预共享密钥为“serverAB”，单击【下一步】按钮。

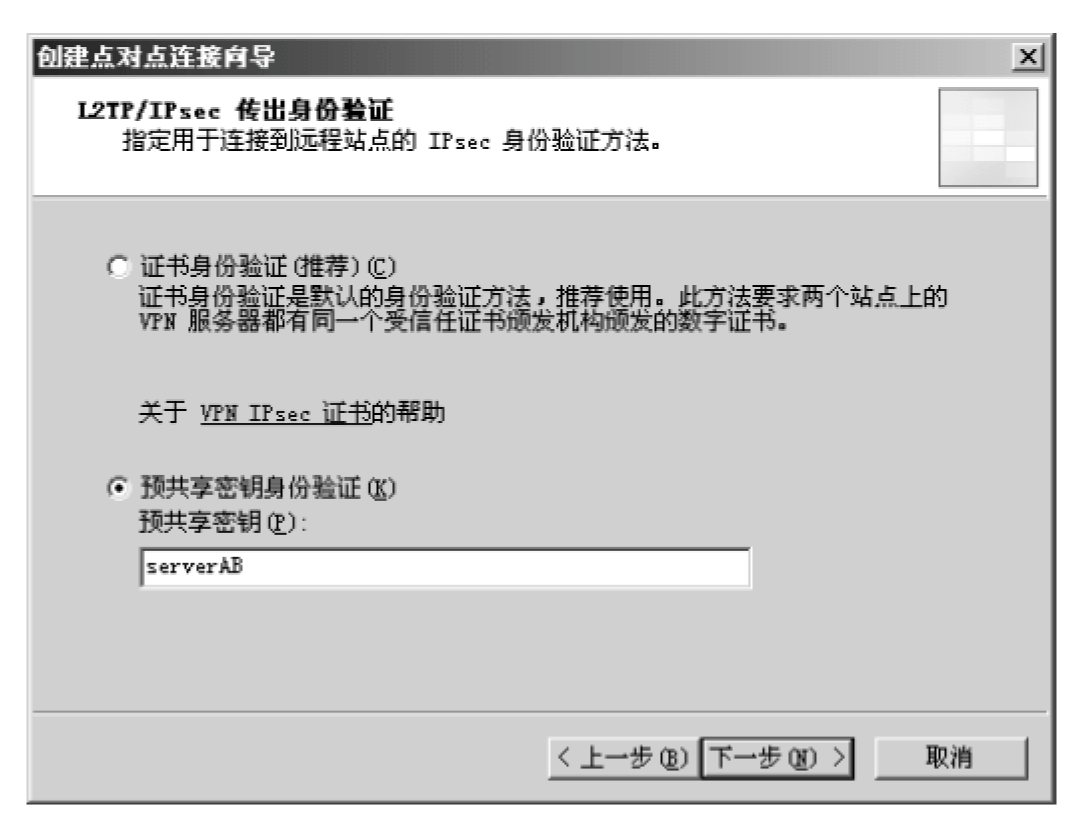


图 16-116

09 弹出【输入 L2TP/IPsec 身份验证】对话框，如图 16-117 所示，在【预共享密钥】文本框中输入“serverAB”，单击【下一步】按钮。

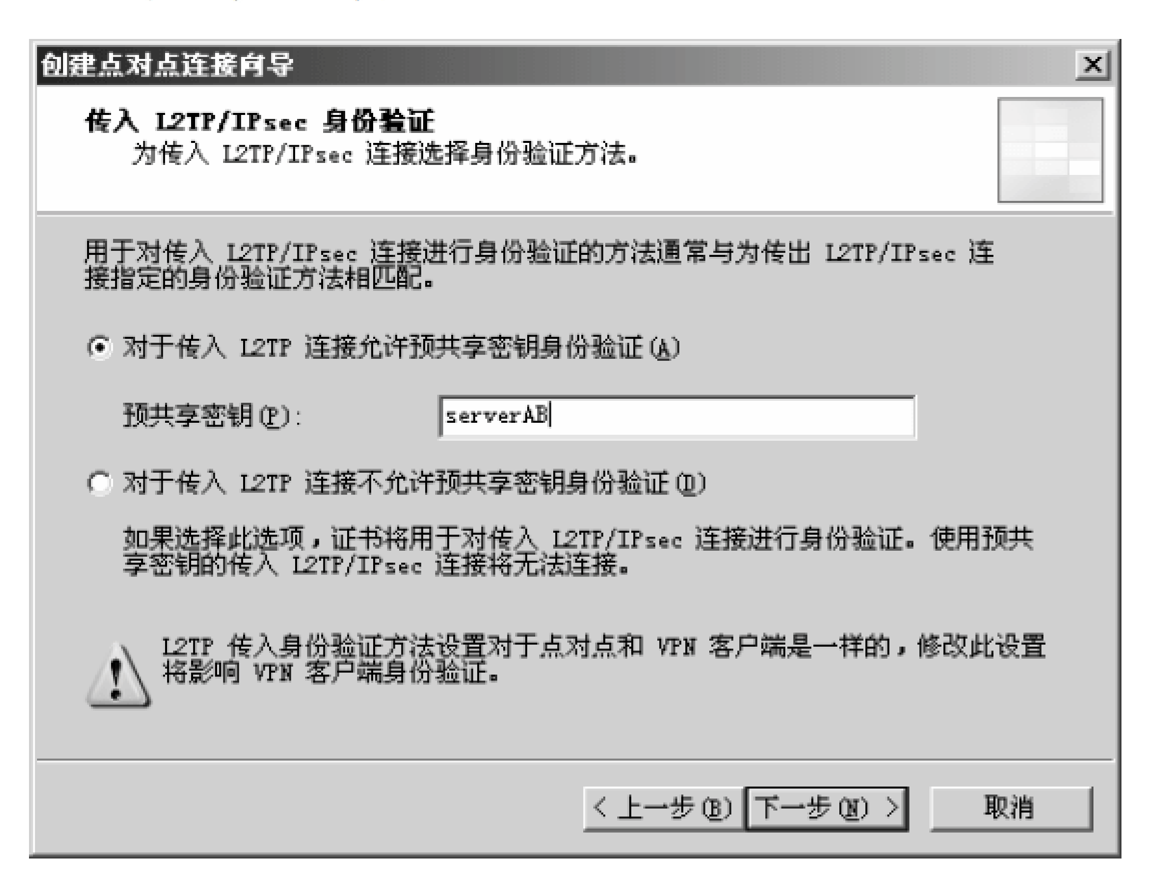


图 16-117

10 弹出【网络地址】对话框，如图 16-118 所示，单击【添加范围】按钮，设置远程站点使用的内部私有地址范围。



图 16-118

11 弹出【IP 地址范围属性】对话框，如图 16-119 所示，在【起始地址】和【结束地址】文本框中输入地址范围“192.168.1.0~192.168.1.255”，单击【确定】按钮。



图 16-119

12 返回【网络地址】对话框，如图 16-120 所示，这时【地址范围】选项列表中已经显示添

加的地址范围，单击【下一步】按钮。



图 16-120

13 弹出【远程 NLB】对话框，如图 16-121 所示，如果使用了负载平衡技术可以使用该配置，本实例不使用，单击【下一步】按钮。

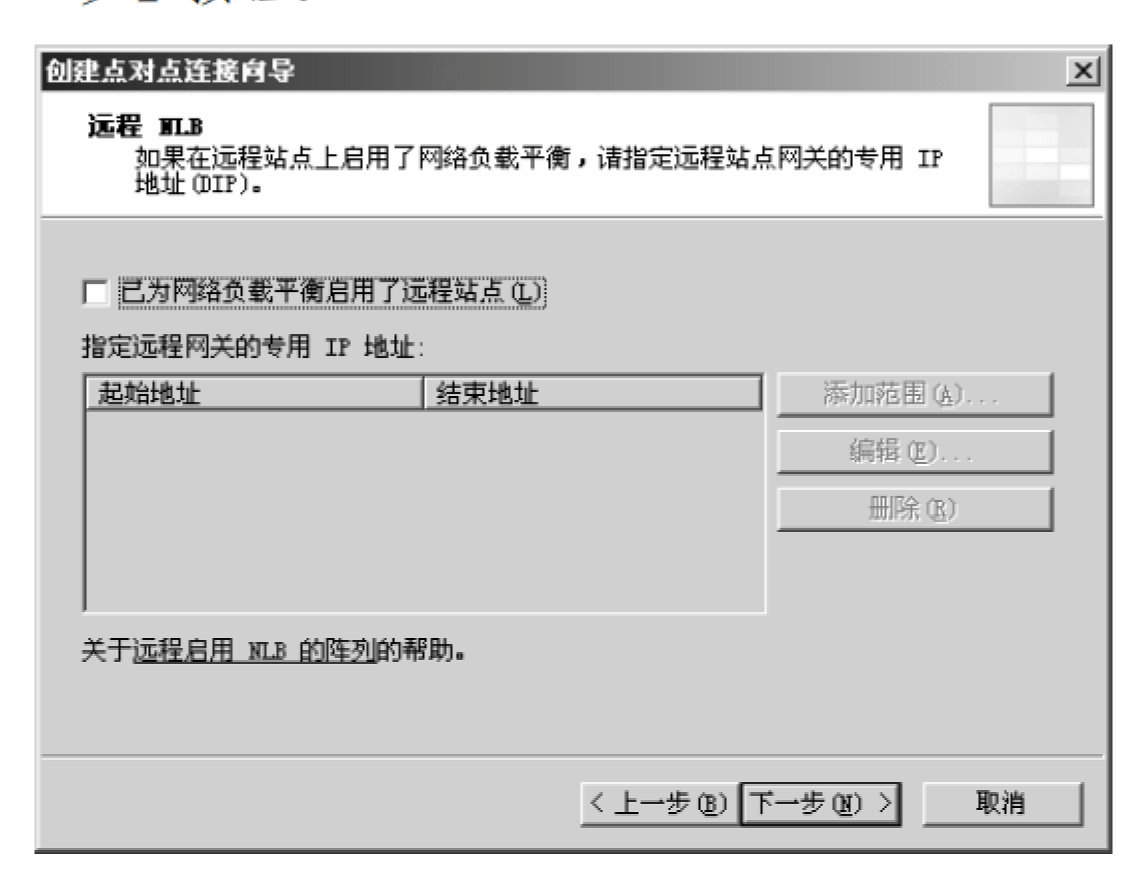


图 16-121

14 弹出【点对点网络规则】对话框，如图 16-122 所示，采用默认配置，单击【下一步】按钮。

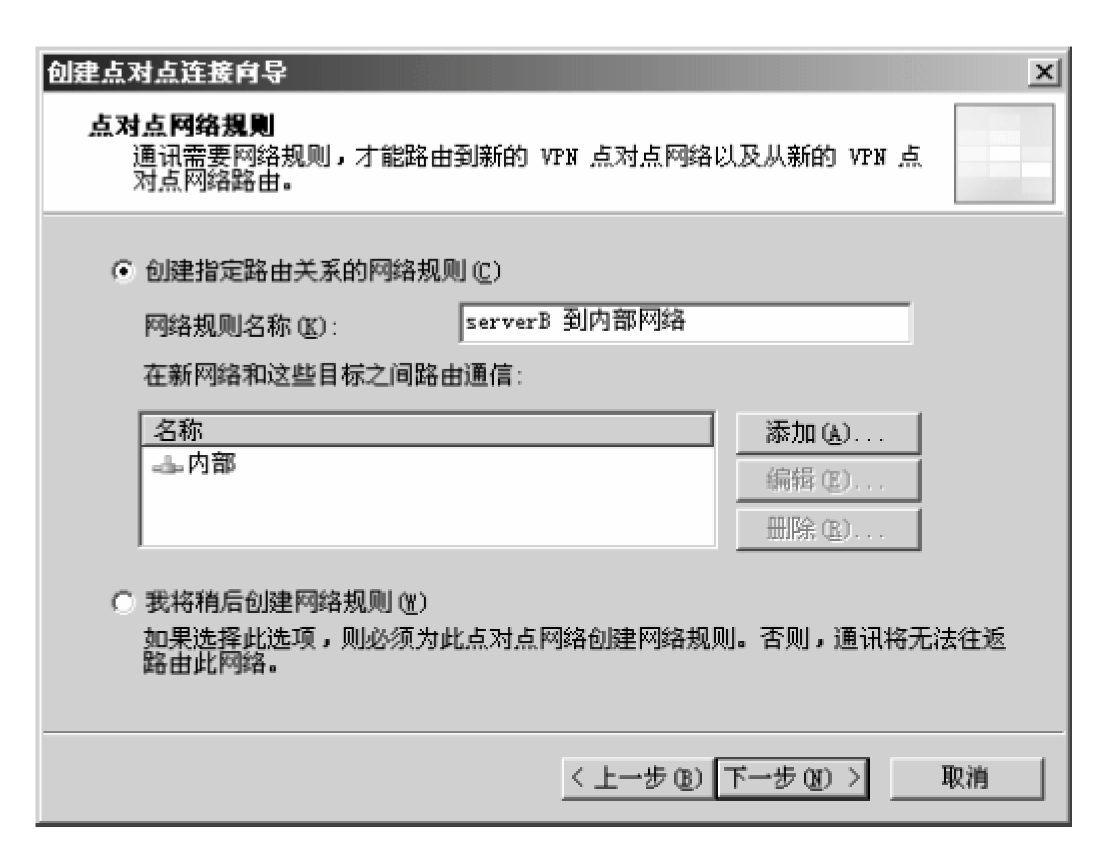


图 16-122

15 弹出【点对点网络访问规则】对话框，如图 16-123 所示，在【将规则应用于这些协议】下拉菜单选项中选择【所有出站通讯】选项，单击【下一步】按钮。

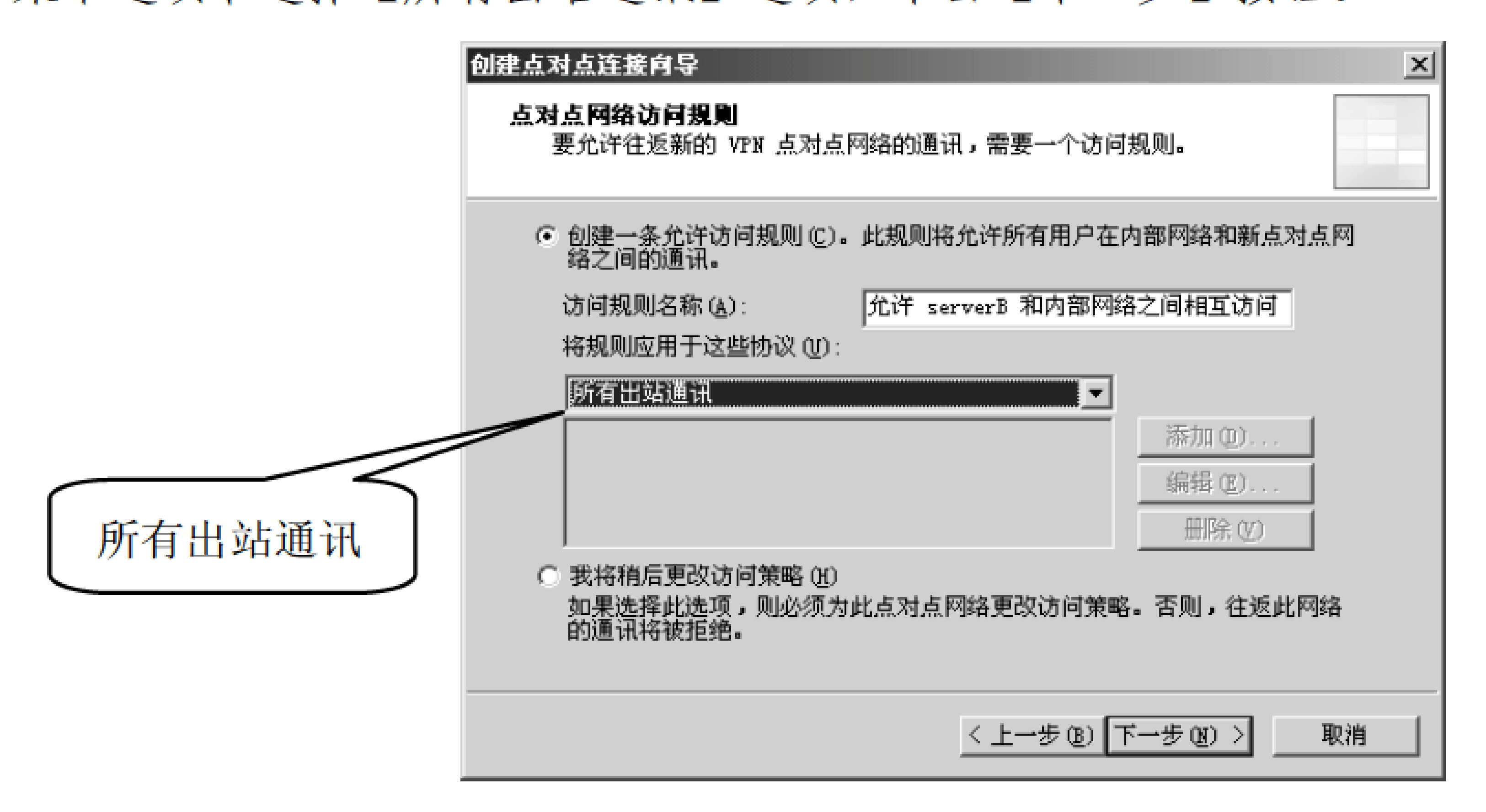


图 16-123

16 VPN 点对点连接配置完成，显示出配置信息，单击【完成】按钮，结束向导，如图 16-124 所示。

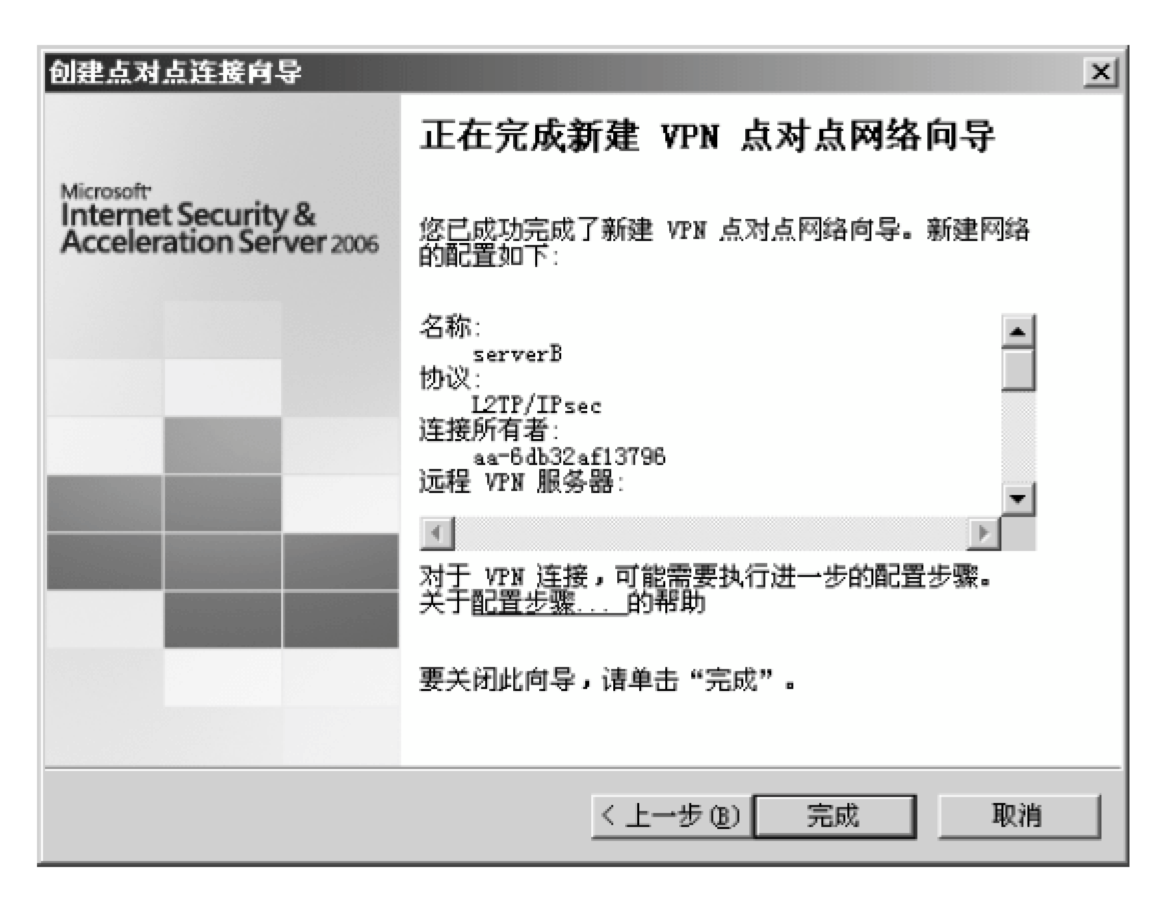


图 16-124

17 弹出【ISA Server 2006】提示框，如图 16-125 所示，远程访问服务重启，单击【确定】按钮。

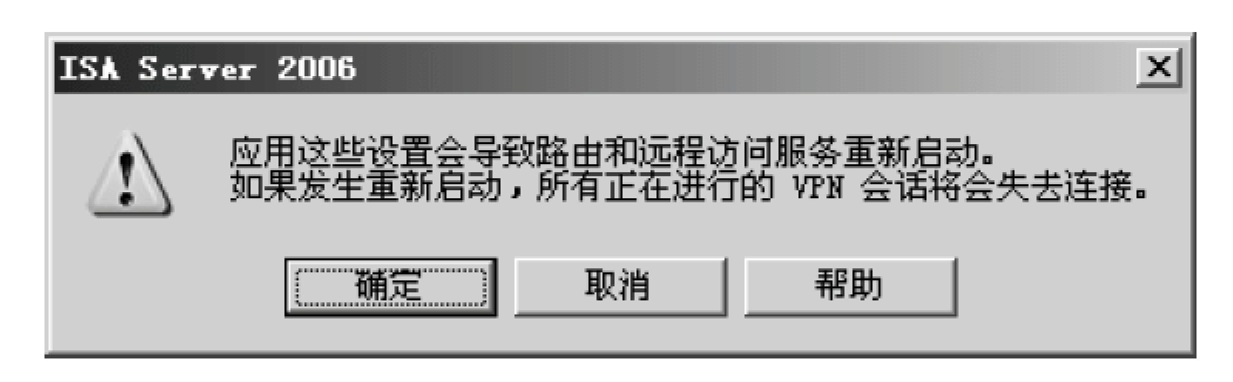


图 16-125

18 弹出【剩余 VPN 点对点任务】提示框，如图 16-126 所示，提示还有哪些 VPN 连接配置没有完成，可按照给出的提示继续配置点对点的 VPN 连接，单击【确定】按钮。



图 16-126

19 弹回程序主界面，在【远程站点】选项卡下显示出新增加的 VPN 连接状态信息，单击【应用】按钮，使配置生效，如图 16-127 所示。



图 16-127

20 在左侧列表中选择【防火墙策略】选项，在右侧【防火墙策略规则】列表中显示了新增的 VPN 流量通信规则，如图 16-128 所示。

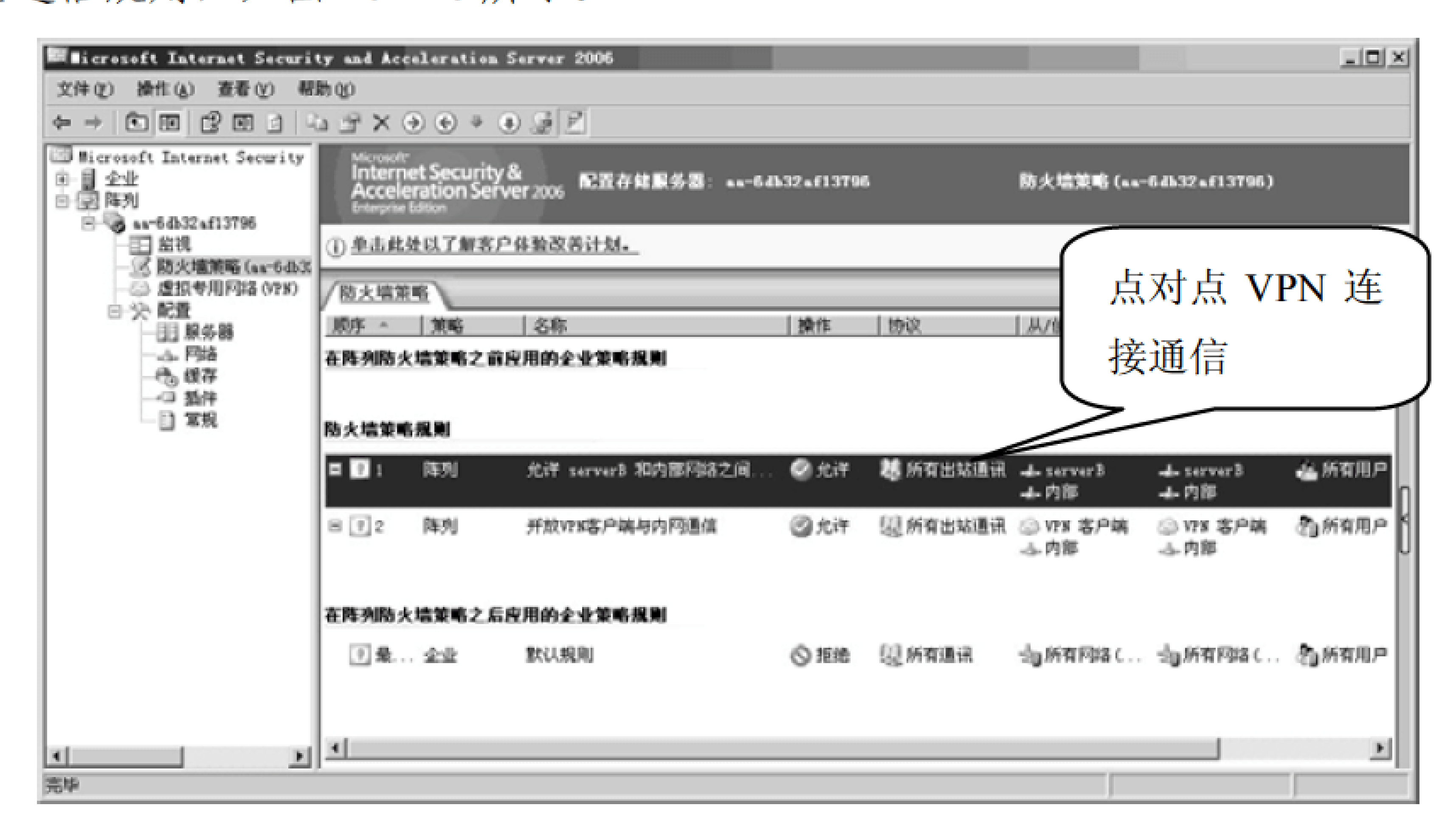


图 16-128

21 在桌面右击【我的电脑】图标，在弹出的快捷菜单中选择【管理】菜单命令，如图 16-129 所示。



图 16-129

22 弹出【计算机管理】窗口，如图 16-130 所示，在左侧选项列表中选择【计算机管理】➢【系统工具】➢【本地用户和组】➢【用户】选项，右击【用户】选项，在弹出的快捷菜单中选择【新用户】菜单命令。



图 16-130

23 弹出【新用户】对话框，如图 16-131 所示，在【用户名】文本框中输入“serverA”，选择【用户不能更改密码】和【密码永不过期】复选框，单击【创建】按钮。

新用户
用户名(U): serverA
全名(F):
描述(D):
密码(P): ******
确认密码(C): ******
用户下次登录时须更改密码(M)
用户不能更改密码(S)
密码永不过期(W)
帐户已禁用(B)
创建(E) 关闭(O)

图 16-131

24 右击 serverA 账户，在弹出的快捷菜单中选择【属性】菜单命令，如图 16-132 所示。



图 16-132

25 如图 16-133 所示，弹出【serverA 属性】对话框，选择【拨入】选项卡，在【远程访问权限】中有三个选项，如果不使用远程访问策略，直接选【允许访问】单选按钮，单击【确定】按钮。

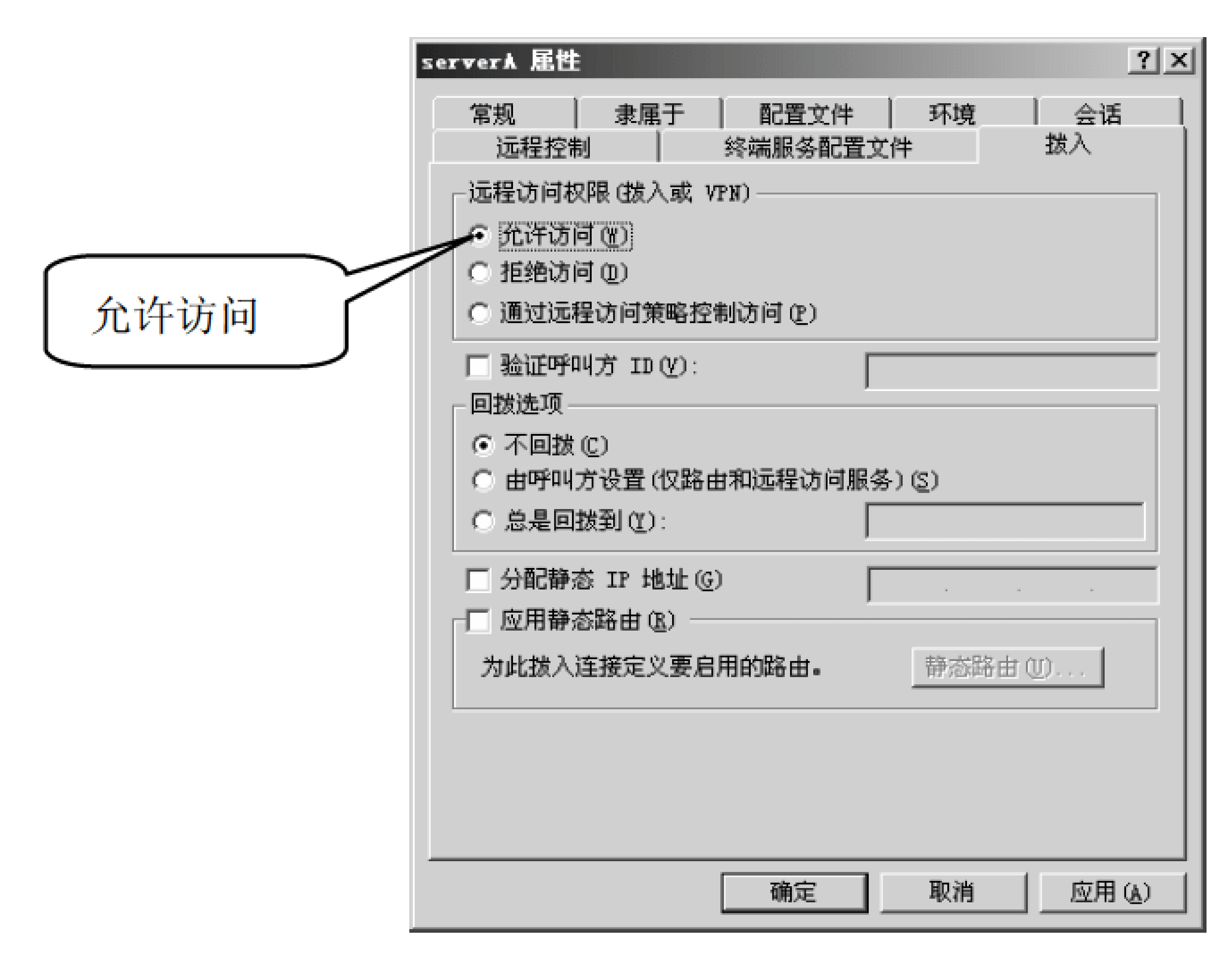


图 16-133

16.4 专家答疑

（1）远程访问 VPN 和远程站点 VPN 两种连接方式，是否适用于所有情况呢？

答：远程访问 VPN 和远程站点 VPN 虽然可以解决大部分人对互联网信息安全传输的需求，但是互联网应用复杂，很多情况下这两种方式是不适用的。

首先，这两种方式需要客户提前支付固定的宽带连接费用，无论使用 VPN 技术传输了多少信息，费用都已经固定了。但是如果信息传输量少，只是偶尔需要进行数据传输，又该如何使用呢？银行的网络是比较特殊的一类，每一天 ATM 机都需要与银行的服务器互连，但是 ATM 机的数量很庞大，如果为所有 ATM 机开放一个固定带宽的宽带接口，那这个费用消耗太大。ATM 机并不需要一直保持 VPN 连接，只需要在用户使用其进行账户业务办理时才需要与服务器进行临时的通信，

而且通信量很小，为了节省开支，银行可以采用按照流量收费的 VPN 方式。

目前银行系统使用的 VPN 技术都是 MPLS VPN。它不但具备 VPN 的普通安全功能，同时还可以实现流量收费业务。

（2）如果远程客户端进行 VPN 连接失败，主要原因有哪些？

答：无论使用哪一种 VPN 连接方式，都需要连接两端使用相匹配的设置，如果配置不匹配，很容易导致连接失败，主要有以下几点匹配项需要注意。

①远程访问策略：如果在访问策略中设置了禁止转发的配置，会直接拒绝连接请求。

②加密认证：VPN 隧道中传输数据时，要进行加密和解密操作，如果两端配置的加密技术不同，也无法实现连通。

③VPN 隧道协议：需要使用 VPN 隧道协议来建立连接，但是基于数据链路层和网络层的隧道协议都有，如果两端选择的不一样，是不可能构成隧道的。如果使用了 IPsec 还需要考虑认证证书的问题，如果认证证书服务器不能正常工作，也会影响 VPN 连接的建立。

④身份验证：在进行 VPN 连接建立时，无论哪种 VPN 技术都需要有身份验证，作为远程访问 VPN 需要配置特定用户允许拨入的权限，如果是远程站点 VPN，除了要有用户权限外，还要考虑两端的身份验证账户配置的是否匹配。

第 17 章　入侵检测系统

随着互联网的逐步普及，网络安全成为了一个首要问题。由于对系统的安全需求也越来越高，入侵检测系统就应运而生了。入侵检测系统是为保证计算机网络系统的安全而设计的，该系统可以及时发现并报告系统中未授权或异常的现象，其作用主要是检测计算机网络中违反安全策略的行为。

17.1　入侵检测系统的概述

除防火墙和杀毒系统的防护外，入侵检测技术也是一种抵御黑客攻击的有效方式。随着入侵检测技术的不断完善和发展，入侵检测产品的市场也越来越大，真正掀起了维护网络安全的热潮。

17.1.1　什么是入侵检测系统

进行入侵检测的软件与硬件的组合便是入侵检测系统，入侵检测系统是主动保护自己免受攻击的一种网络安全系统，作为防火墙的合理补充，入侵检测系统能够帮助系统对付网络的攻击，这就在一定程度上提高了系统管理员的安全管理能力，包括安全审计、监视、攻击识别和响应等，也提高了信息安全基础结构的完整性。

通过使用入侵检测软件，收集计算机网络或计算机系统中的若干关键点的信息，并对这些信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。

17.1.2　入侵检测系统的基本功能与组成

一个合格的入侵检测系统能大大简化网络管理员的工作，保证网络安全的运行。因此，入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时防护，还能给网络安全策略的制定提供指南。

更为重要的一点是，它管理、配置简单，从而使非专业人员非常容易地实现网络安全。而且，它的规模还可根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时做出响应，包括切断网络连接、记录事件和报警等。

具体来说，入侵检测系统的主要功能有。

（1）监测并分析用户和系统的活动。

（2）核查系统配置和漏洞。
（3）评估系统关键资源和数据文件的完整性。
（4）识别已知的攻击行为。
（5）统计分析异常行为。
（6）操作系统日志管理，并识别违反安全策略的用户活动。

入侵检测系统是用来检测网络系统，或者更广泛意义上的信息系统中的非法攻击。入侵检测系统主要由如下 4 个部分组成。

（1）数据收集装置：收集反映状态信息的审计数据。
（2）检测器：负责分析和检测入侵，并发出警告信息。
（3）知识库：提供必要的数据信息支持。
（4）控制器：根据警告信息，人工或自动做出相应动作。

其系统结构如图 17-1 所示。

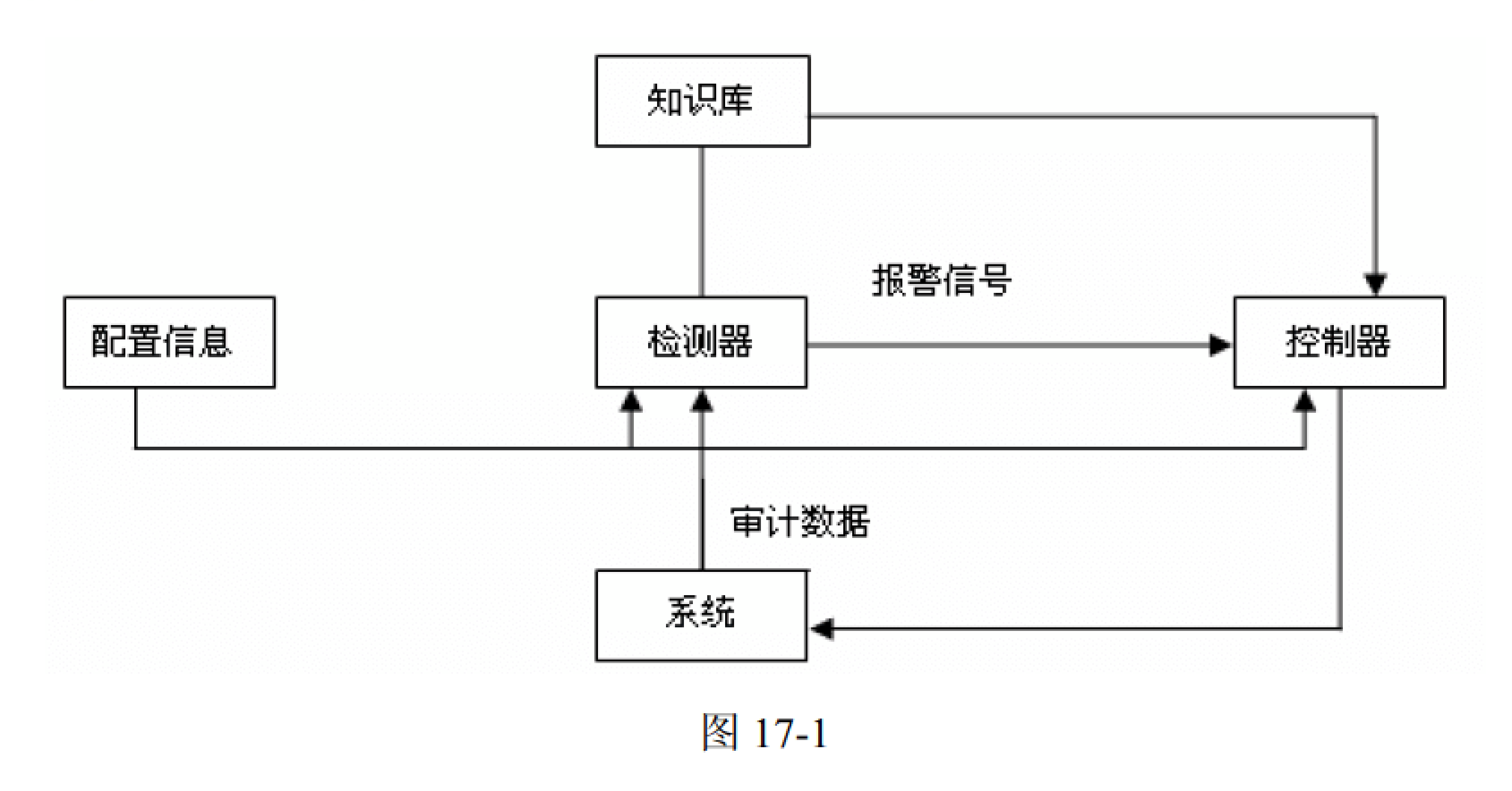


图 17-1

17.1.3 入侵检测系统的发展方向

入侵检测系统可以弥补防火墙的不足，为网络提供实时的监控，并且在发现入侵初期就采取相应的防护手段，目前入侵检测系统已经被大多数组织机构所接受。由于入侵检测系统存在着一些问题，所以其发展方向也成为大家关注的热点。

1. 分析技术的改进

分析技术的改进可以解决入侵检测系统的误报和漏报问题。目前入侵检测分析方法主要有统计分析、模式匹配、数据重组、协议分析、行为分析等几种。

（1）统计分析：统计网络中相关事件发生的次数，达到判断攻击的目的。
（2）模式匹配：利用对攻击的特征字符进行匹配完成对攻击的检测。
（3）数据重组：对网络连接的数据流进行重组再加以分析，而不只是分析单个数据包。
（4）协议分析技术：在对网络数据流进行重组的基础上，理解并应用协议，利用模式匹配和统计分析的技术来判断攻击是否存在。利用该项技术可以有效降低误报和漏报概率。

（5）行为分析技术:该技术不仅简单分析单次攻击事件，还根据前后发生的事件确认是否确有攻击发生，攻击行为是否生效。它是入侵检测分析技术的最高境界，由于算法处理和规则制定的难度很大，目前还不是非常成熟，但却是入侵检测技术未来发展的趋势。

目前最好综合使用多种检测技术，而不只是依靠传统的统计分析和模式匹配技术。另外，规则库是否及时更新也会影响检测的准确程度。

2. 内容恢复和网络审计功能的引入

由于入侵检测的最高境界是行为分析，但行为分析目前还不是很成熟，所以有的入侵检测产品中就引入了内容恢复和网络审计两项功能。

（1）内容恢复：在协议分析的基础上，对网络中发生的行为加以完整的重组和记录，所以网络中发生的任何行为都逃不过它的监控。

（2）网络审计：是对网络中所有的连接事件进行记录。入侵检测的接入方式决定入侵检测系统中的网络审计。不仅可以像防火墙那样记录网络进出信息，还可记录网络内部连接状况。该功能对内容无法恢复的加密连接尤其有用。

内容恢复和网络审计可以帮助网络管理员了解到网络的真正运行状况，其实就是调动网络管理员参与行为分析过程。这样网络管理员不仅可以看到孤立的攻击事件的报警，还可以看到整个攻击过程、了解攻击确实发生与否、查看攻击者的操作过程以及攻击造成的危害。不但可以发现已知攻击，还可以发现未知攻击。但使用此功能需注意对用户隐私的保护。

3. 集成网络分析和管理功能

入侵检测不仅检测网络攻击，同时还可以收到网络中的所有数据，对网络的故障分析与管理也起到重大作用。入侵检测不应只采用被动分析方法，最好能和主动分析技术相结合。所以，入侵检测产品集成网管、扫描器、嗅探器等功能是其以后发展的方向。

4. 安全性和易用性的提高

入侵检测系统本身就是一个安全产品，其自身安全极为重要。所以目前的入侵检测产品大多采用硬件结构、黑洞式接入等方式来确保自身的安全。同时，对易用性的要求也日益增强，例如：全中文的图形界面，自动的数据库维护，多样的报表输出，这些都是优秀入侵检测产品的特性和以后继续发展的趋势。

5. 改进对大量网络数据的处理方法

随着大量网络数据的出现，对入侵检测的性能要求也逐步提高，出现了千兆入侵检测等产品。但如果入侵检测检测产品既要具备攻击分析，同时又要具备内容恢复和网络审计功能，则其存储系统也很难完全工作在千兆网络环境下。在这种情况下，网络数据分流是一个很好的解决方案，这也是国际上较通用的一种作法。

6. 防火墙联动功能

防火墙联动功能是指当入侵检测发现攻击时，将攻击信息自动发送给防火墙，防火墙加载动

态规则拦截入侵。但如果无限制使用联动（如未经充分测试）会对防火墙的稳定性和网络应用造成负面影响。

17.1.4 入侵检测系统的缺陷

入侵检测系统有如此重大的作用，但在国内的应用还远远没有普及，一方面是由于用户的认知程度较低，另一方面是因为入侵检测是一门比较新的技术，不是所有厂商都具有研发入侵检测产品的实力。

目前的入侵检测产品大多存在如下几个问题。

（1）误报、漏报率高。入侵检测系统对网络上所有的数据进行分析，如果攻击者对系统进行攻击尝试，而系统相应服务开放，只是漏洞已经修补，那么这一次攻击是否需要报警，就是一个需要检测系统判断的问题。但大量的报警事件会分散管理员的精力，反而无法对真正的攻击做出反映。和误报相对应的是漏报，随着攻击的方法不断更新，入侵检测系统是否能报出网络中所有的攻击也是一个问题。

（2）产品适应能力低。传统入侵检测系统产品在开发时没有考虑特定网络环境的需求。随着网络技术的不断发展，网络设备也变得复杂化、多样化，这就需要入侵检测产品能动态调整，以适应不同环境的需求。

（3）大型网络的管理问题。现在企业规模在不断扩大，对入侵检测系统产品的需求从单点发展到跨区域甚至全球，这就使公司把产品的管理问题提上日程。首先需要确保新的产品体系结构能够支持数以百计的入侵检测系统传感器；还要能够处理传感器产生的告警事件；最后还要解决攻击特征库的建立、配置以及更新问题。

（4）缺少防御功能检测。由于入侵检测系统是采取被动监听的方式发现网络问题，无法主动发现网络中的安全隐患和故障。如何解决这个问题也是入侵检测产品面临的挑战，所以需要在下一代入侵检测系统产品中嵌入防御功能，才能变被动为主动。

（5）评价入侵检测系统产品没有统一标准。对入侵检测系统的评价目前还没有统一的标准，使入侵检测系统之间不易互联。随着技术的发展和对新攻击识别的增加，入侵检测系统需要不断升级才能保证网络的安全性。

（6）处理速度上的瓶颈。随着高速网络技术如 ATM、千兆以太网等的相继出现，入侵检测产品能否高效处理网路中的数据，也是衡量入侵检测产品的重要依据。如何实现高速网络下的实时入侵检测是急需解决的问题，因为目前的百兆、千兆入侵检测系统产品的性能指标，与实际要求还存在很大的差距。

17.2 入侵检测系统的分类

根据监测对象不同，入侵检测系统可分为多种，常见的有基于主机的入侵检测、基于网络的入侵检测、误用入侵检测和混合性入侵检测等，下面就对这几种典型的入侵检测系统进行介绍。

17.2.1　基于主机的入侵检测系统

基于主机的入侵检测系统是早期的入侵检测系统结构，其检测的目标主要是主机系统和本地用户系统。在这种环境下，入侵检测的任务被大大简化。检测原理是根据主机的审计数据和系统日志发现可疑事件，给出关于怀疑为不安全行为的报告。检测系统可以运行在被检测主机或单独主机上，系统结构如图 17-2 所示。

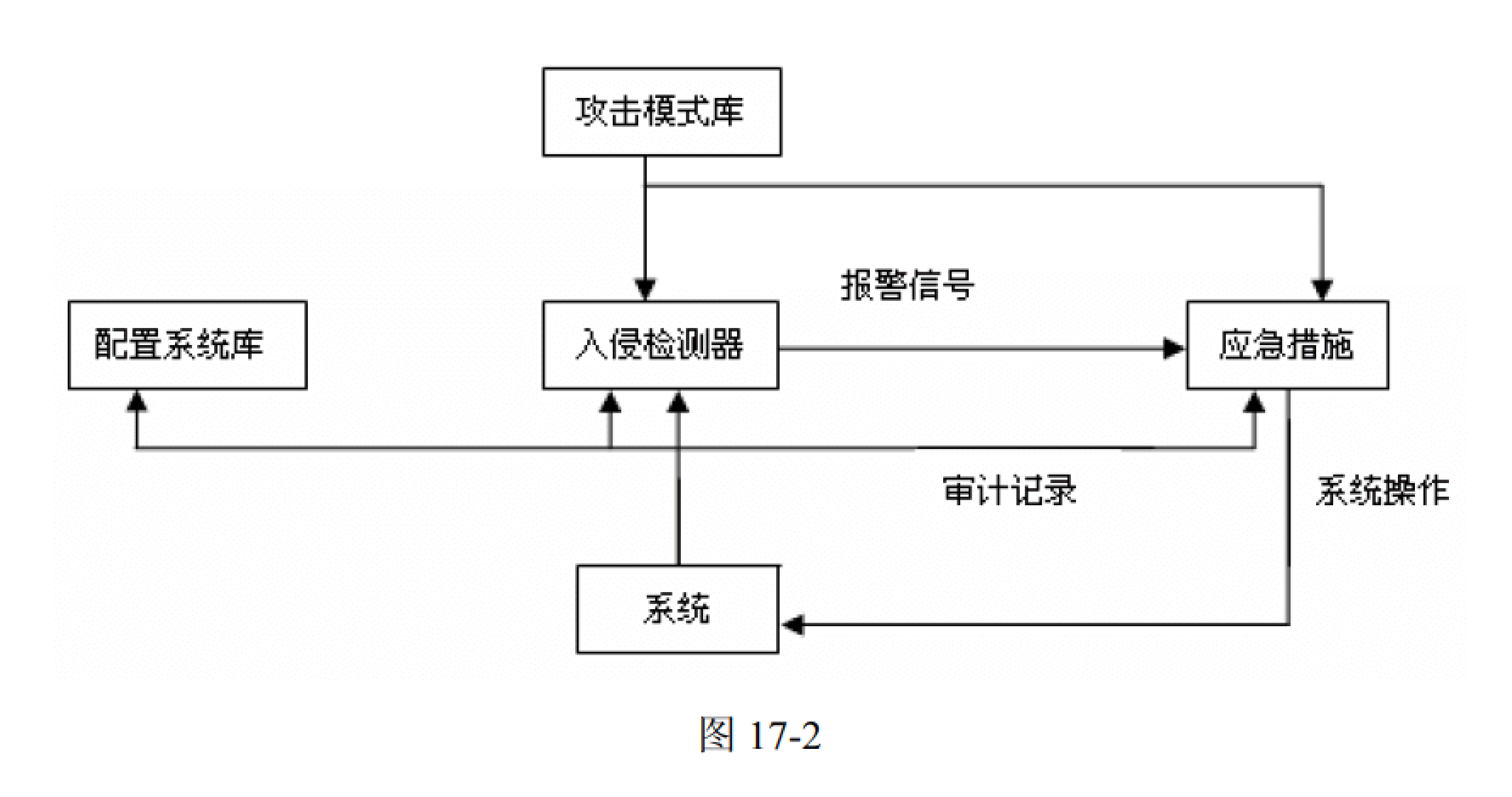


图 17-2

两种主要基于主机的入侵检测类型是：

（1）网络监视器。它监视主机的网络连接，并试图判断这些连接是否是一个威胁。并可检查出网络连接表达的一些试图进行的入侵类型。记住，这与基于网络的入侵检测不同，因为它只监视它所运行的主机上的网络通信，而不是通过网络的所有通信。基于此种原因，它不需要网络接口处于混杂模式。

（2）主机监视器。它监视文件、文件系统、日志或主机其他部分，查找特定类型的活动，进而判断是否是一个入侵企图（或一个成功的入侵）之后，通知系统管理员。

基于主机入侵检测的优点主要体现在：当主机数量较少时，该种方法的性能价格比较高；该种方法可以很容易检测一些活动，而这些活动很难在基于协议的系统中被发现；如果黑客得到用户的主机名和密码后，基于主机的代理是很容易区别正常活动和非法活动的；每个主机有其自己的代理，用代理的方式一般不会因为网络流量的增加而丢掉对网络行为的监控。

其缺点在于：由于操作系统平台提供的日志信息格式不同，必须针对不同的操作系统安装不同的入侵检测系统。如果入侵者通过其他系统漏洞入侵系统并取得管理者的权限，那将会导致主机型入侵检测系统失效；会因分布式（Denail of Service，DoS）攻击而失效；当监控分析时会增加该台主机的系统资源负荷，从而影响被监测主机的性能，甚至成为入侵者利用的工具使被监测的主机因为负荷过重而死机。

17.2.2　基于网络的入侵检测系统

基于网络入侵检测是通过分析主机之间网线上传输的信息来工作的。它是利用一个工作在混杂模式（Promiscuous Mode）下的网卡，来实时监视并分析通过网络的数据流。它的分析模块通常

使用模式匹配、统计分析等技术来识别攻击行为，其结构如图 17-3 所示。

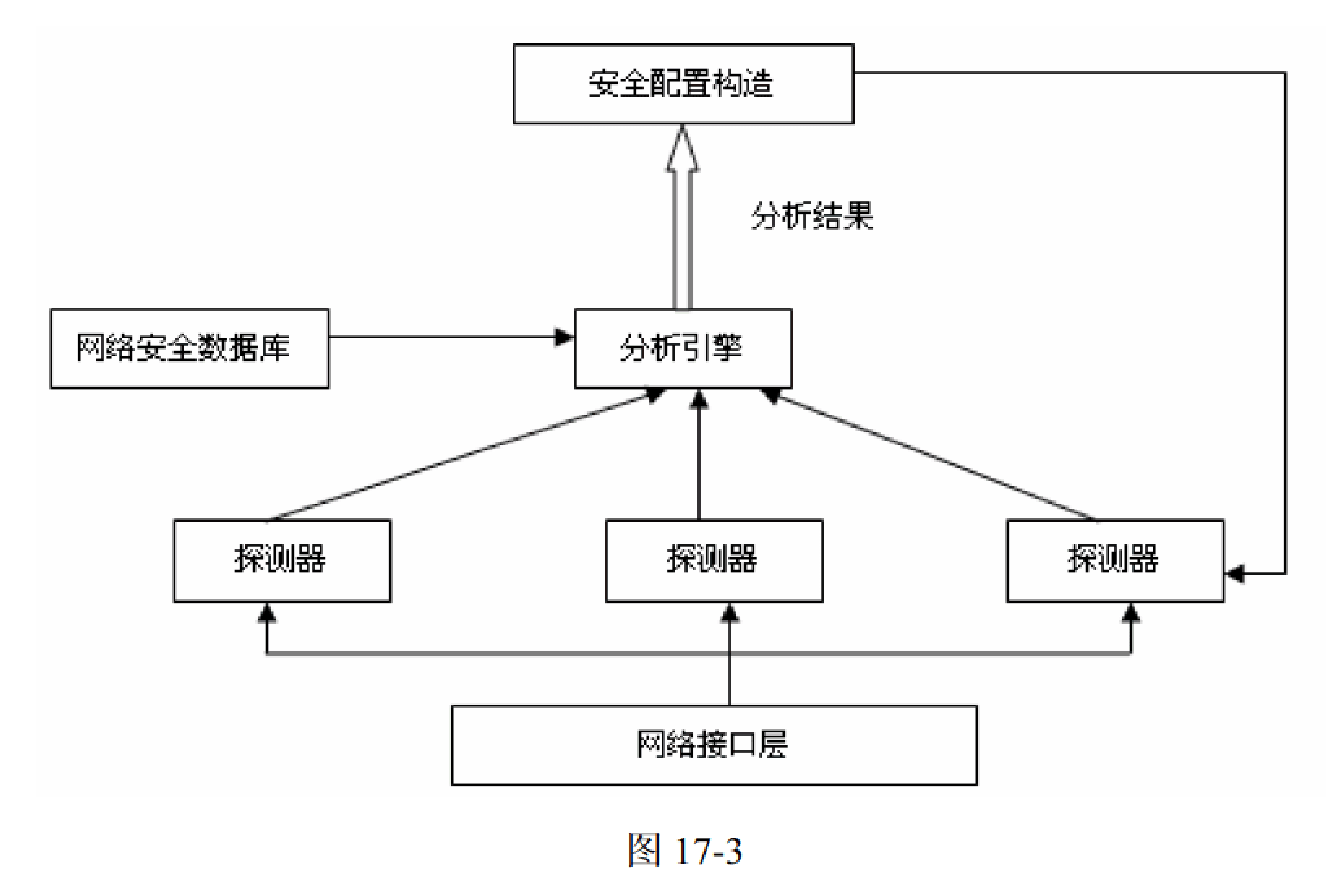


图 17-3

这种类型的系统放置在网络上，靠近该系统或者系统群，它们检查网络通信并判断是否在可接受的范围内。基于网络的入侵检测系统监视整个网络的通信。

网络接口卡（NIC）可以在如下两种模式下工作：

（1）正常模式。需要发送到计算机（通过包的以太网或 MAC 地址进行判断）的数据包，通过该主机系统进行中继转发。

（2）混杂模式。此时以太网上所能见到的数据包都向该主机系统中继。一块网卡可以从正常模式向混杂模式转换，通过使用操作系统的底层功能就能直接告诉网卡进行如此改变。通常，基于网络的入侵检测系统要求网卡处于混杂模式。

基于网络的入侵检测系统的探测器可以按一定的规则从网络上获取与安全事件相关的数据包，分析引擎从探测器上接收到的数据包结合网络安全数据库进行分析，最后把分析的结果传递给配置构造器，配置构造器根据分析引擎器的结果构造出探测器所需要的配置规则。一旦检测到了攻击行为，网络入侵系统中的响应模块就做出响应，比如报警、切断相关用户的网络连接等。不同入侵检测系统在实现时采用的响应方式也不同，但通常都包括通知管理员、切断连接、记录相关的信息等。

基于网络入侵检测的优点表现在：成本低、检测速度快；可以检测到主机型检测系统检测不到的攻击行为；可以作用在网络的边缘上，即攻击还没能接入网络时就被制止；不影响操作系统的性能，不占用任何资源；架构网络型入侵检测系统简单。其缺点是：如果网络流速高时可能会丢失许多数据包，容易让入侵者有机可乘；无法检测加密的数据包；无法检测出直接对主机的入侵。

17.2.3　误用入侵检测系统

误用检测（Misuse detection）又称特征检测（Signature-based detection），误用入侵检测系统的应用是建立在对过去各种网络入侵的方法和系统缺陷上。它需要建立一个数据库，再在各种收集到的网络活动信息中寻找与数据库项目相关的蛛丝马迹。当符合条件的信息被发现后，就会触发一个

警告，即任何不符合匹配条件的信息将会被认为合法，尽管其中可能包含隐蔽入侵的行为。所以误用检测系统具备较高准确性，但其完整性则由数据更新速度来确定。

设定一些入侵活动的特征（Signature），通过比较现在的活动是否与这些特征匹配来检测。

常用的检测技术有如下几种：

（1）专家系统：采用一系列的检测规则分析入侵的特征行为。不同的系统与设置具有不同的规则，且规则之间无通用性。专家系统的建立依赖于知识库的完备性，而知识库的完备性又由审计记录的完备性与实时性决定。入侵的特征抽取与表达，是入侵检测专家系统的关键。在系统实现中，将有关入侵的知识转化为 if-then 结构（也可以是复合结构），if 部分为入侵特征，而 then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全由专家系统知识库的完备性决定。

（2）基于模型的入侵检测方法：入侵者在攻击系统时一般采用一定的行为序列，如猜测口令的行为序列。这种行为序列构成了具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时检测出恶意的攻击。基于模型的入侵检测方法可以只监测一些主要的审计事件。当这些事件发生后，再开始记录详细的审计，从而减少审计事件处理工作。这种检测方法的优点是可以检测组合攻击（coordinate attack）和多层攻击（multi-stage attack）两种攻击方式。

（3）简单模式匹配（Pattern Matching）：基于模式匹配的入侵检测方法将已知入侵特征编码成为与审计记录相符合模式。当新审计事件产生时，将寻找与其相匹配的已知入侵模式。

（4）软计算方法：软计算方法包含了神经网络、遗传算法与模糊技术。

不难看出，误用入侵检测系统的优点是：具有非常高的准确率，同时检测匹配条件可以很清楚地描述，从而有助于网络管理员采取相应的预防措施。一个比较明显的缺点在于：收集所有已知或发现的攻击行为和系统脆弱性信息比较困难。

17.2.4　混合性入侵检测

主机型和网络型两种入侵检测系统都有各自的优缺点，而混和入侵检测系统是基于主机和网络的入侵检测系统的结合。许多机构的网络安全解决方案都同时采用了基于主机和基于网络的两种入侵检测系统，因为这两种系统在很大程度上互补，两种技术结合可以大幅度提升网络和系统面对攻击和错误使用时的抵抗力，使安全措施更加有效。

17.3　项目实施 1：入侵检测系统工具实战

在了解了什么是入侵检测技术、入侵检测的技巧和相关分类后，下面再来介绍一些具体使用入侵检测技术的范例，从而帮助用户更好地保护计算机和网络安全。目前，常用的入侵检测系统有 Sax 入侵检测系统、BlackICE 入侵检测系统等，使用这些系统可以积极主动地保护网络安全。

17.3.1　异常入侵检测系统

异常检测是检测入侵者异常于正常主体的活动。根据这一理念建立主体正常活动的【活动简

档】，将当前主体的活动状况与【活动简档】相比较，当违反其统计规律时，认为该活动可能是【入侵】行为，即任何不符合以往活动规律的行为都将被视为入侵行为。所以异常入侵系统的检测能力是很高的，但是要保证其具有很高的正确性就很困难了。

统计方法是当前入侵检测系统中常用的方法，是一种成熟的入侵检测方法。可以使入侵检测系统了解到目标计算机的日常行为，将那些与正常活动之间存在较大统计偏差的活动标识成为异常活动。常用的入侵检测统计模型有如下几种：

（1）操作模型：该模型假设异常可通过测量结果与一些固定指标相比较得到，而固定指标可根据经验值或一段时间内的统计得到，如在短时间内多次失败的登录可能是口令尝试攻击。

（2）方差：计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时就有可能是出现异常。

（3）多元模型：操作模型的扩展，通过同时分析多个参数实现检测。

（4）马尔柯夫过程模型：将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化。当一个事件发生时，该状态矩阵发生转移的概率较小的可能是异常事件。

（5）时间序列分析：将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是黑客入侵。

异常检测的优点表现在：具有抽象系统正常行为从而检测系统异常行为的能力。这种能力不受系统是否知道该种入侵的限制，所以能够检测新的入侵行为。另外，对于合法用户超越其权限的违法行为的检测能力大大加强。其缺点是：如果入侵者了解到检测规律，就可以小心地避免系统指标的突变，而使用逐渐改变系统指标的方法逃避检测。另外，检测效率也不高。最重要的是，异常检测是一种【事后】检测，当检测到入侵行为时，破坏早已经发生了。

17.3.2　使用 Sax 入侵检测系统

Sax 入侵检测系统是一种积极主动的网络安全防护工具，提供了对内部和外部攻击的实时保护，它通过对网络中所有传输的数据进行智能分析和检测，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，在网络系统受到危害之前拦截和阻止入侵。

1. 设置 Sax 入侵检测系统

在使用 Sax 入侵检测系统来防护系统或网络安全之前，还需要对该软件的相关功能进行设置，以便更好地保护系统安全。

设置 Sax 入侵检测系统的操作步骤如下。

01 下载并安装 Sax 入侵检测系统，安装完毕后双击桌面上的快捷图标或选择【开始】➢【所有程序】➢【Sax 入侵检测系统】菜单命令，打开其主界面，包括按节点浏览、运行状态以及统计项目 3 个部分，如图 17-4 所示。



图 17-4

02 选择【监控】➢【常规设置】菜单命令，打开【设置】对话框，如图 17-5 所示，在【常规设置】选项卡中可对数据包缓冲区大小和从驱动程序读取数据包的最大间隔时间进行设置。



图 17-5

03 在【设置】对话框中选择【适配器设置】选项卡，如图 17-6 所示，在该选项卡中选择相应的网卡，因为该检测系统是通过适配器来捕捉网络中正在传输的数据，并对其进行分析，所以正确选择网卡是能够捕捉到入侵的关键一步。



图 17-6

04 在【Sax 入侵检测系统】主界面中选择【设置】➢【别名设置】菜单命令，打开【别名设置】对话框，如图 17-7 所示，在其中可对物理地址、IP 地址、端口进行各种操作，如添加、编辑、删除、导出等。

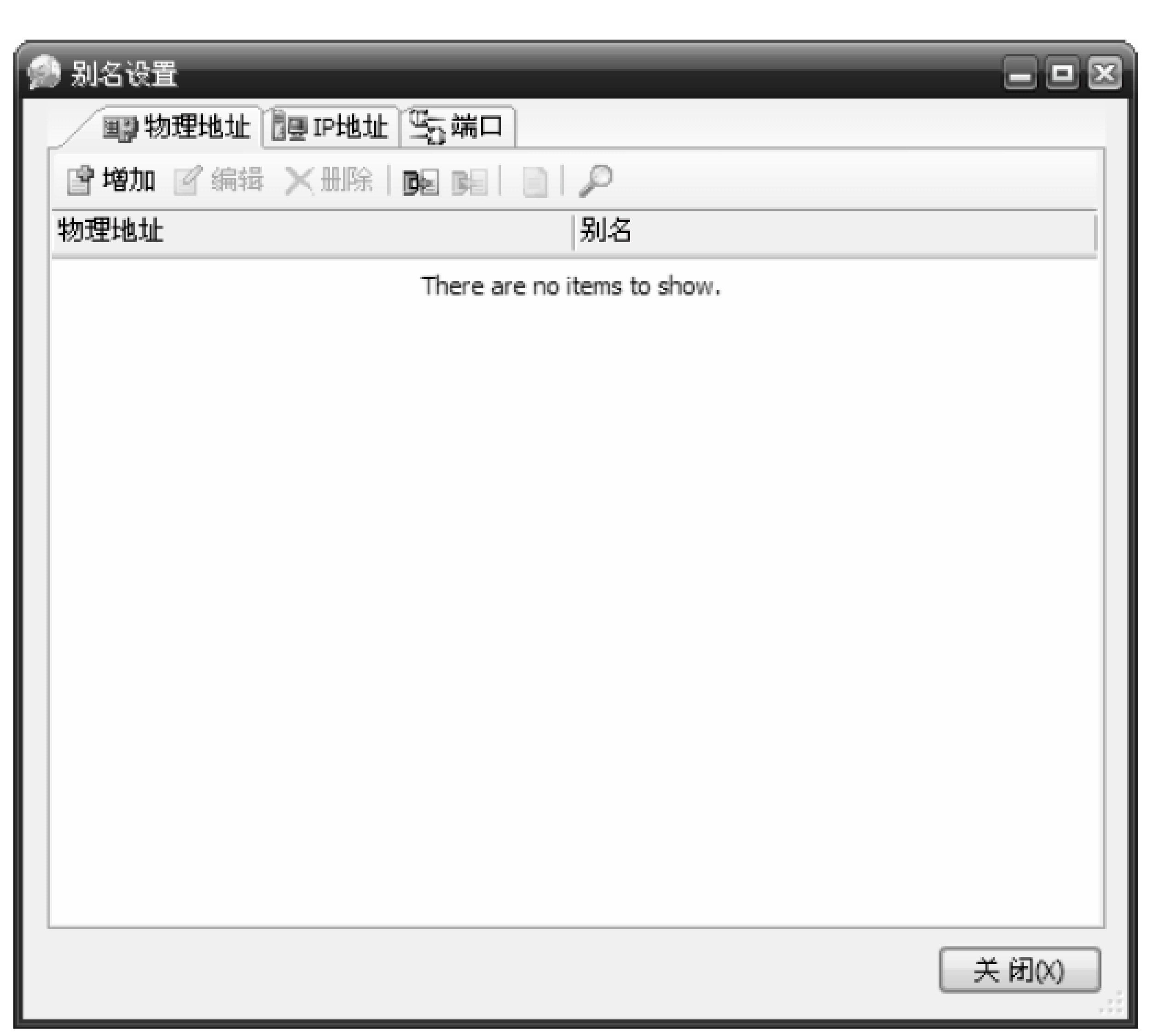


图 17-7

05 选择【设置】➢【安全策略设置】菜单命令或单击工具栏中的【安全策略】按钮，打开【安全策略】对话框，如图 17-8 所示，在其中对当前选中的策略进行相应的操作，如衍生、查看、启用、删除、导入、导出和升级等。



图 17-8

06 选择【设置】➢【专家检测设置】菜单命令或单击工具栏中的【专家检测】按钮，打开【专家检测设置】对话框，在其中对网络中的所有通信数据进行专家级的智能化的分析，并报告入侵事件，如图 17-9 所示。



图 17-9

07 选择【设置】➢【选项】菜单命令或单击工具栏中的【选项】按钮，打开【选项】对话框，如图 17-10 所示，选择【显示】功能项，在其中对是否启用物理地址、IP 地址和端口别名进行设置。



图 17-10

08 如图 17-11 所示，选择【响应方案设置】功能项，在其中对响应方案进行增加、删除或修改操作。系统提供了【仅记录日志】、【阻断并记录日志】和【干扰并记录日志】三种默认的响应方案，它们是不能被删除的，但是可以修改。



图 17-11

09 单击【增加】或【修改】按钮，打开【定义响应方案】对话框，如图 17-12 所示，在其中对响应方案进行具体设置，包括名称、响应动作和阻断会话方式（只有选择了【阻断会话】才可以设置阻断会话方式）。

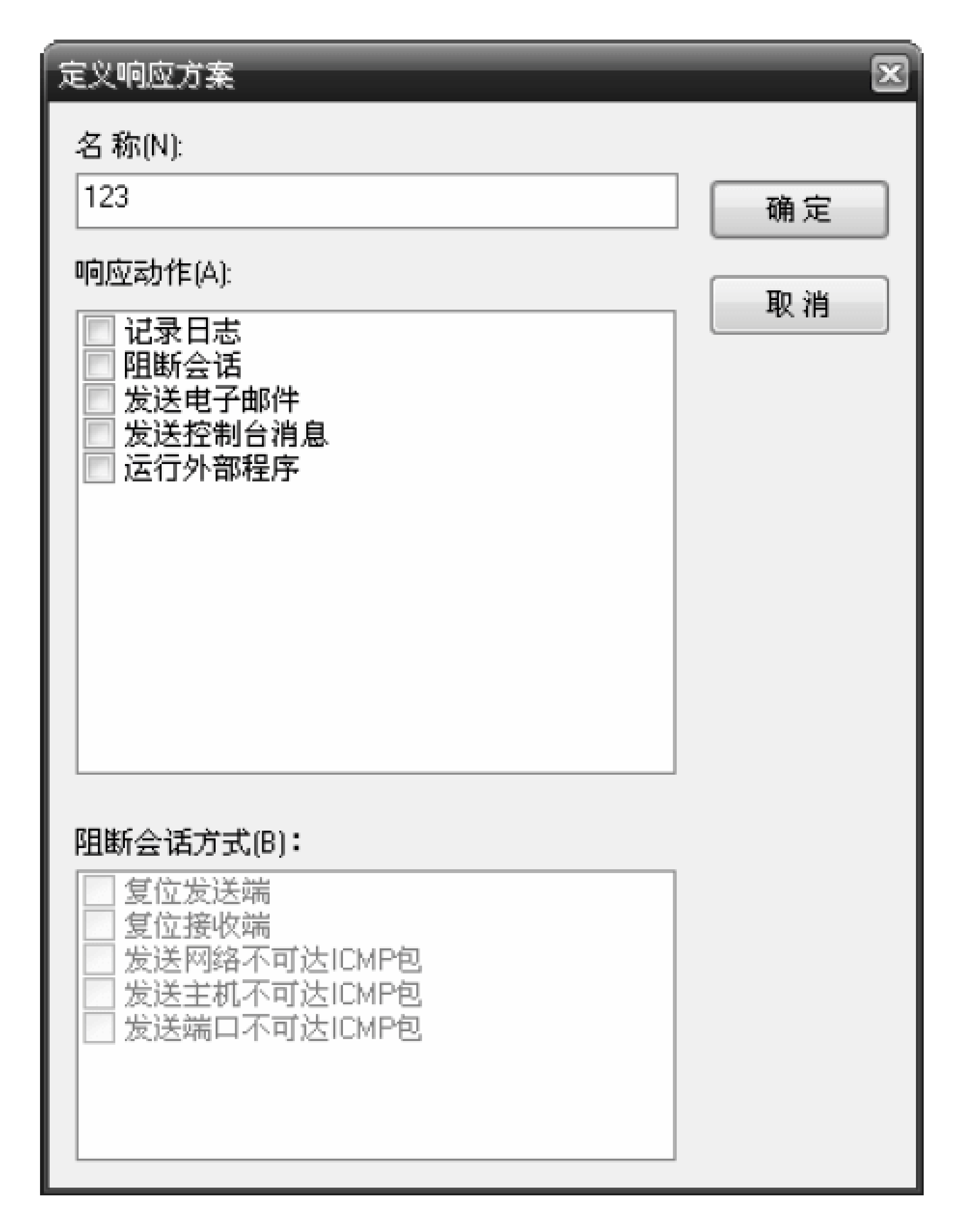


图 17-12

10 选择【响应设置】➢【邮件】功能项，在其中可以对发送邮件所使用的服务器、账号、密码、接收人(多个接收人用分号分隔)和邮件正文进行设置，如图 17-13 所示。



图 17-13

11 选择【响应设置】➢【发送控制台消息】功能项，在其中可以对将接收消息的目标主机的 IP 地址和消息正文（发送主机和接收主机必须安装【Messenger】服务）进行设置，如图 17-14 所示。

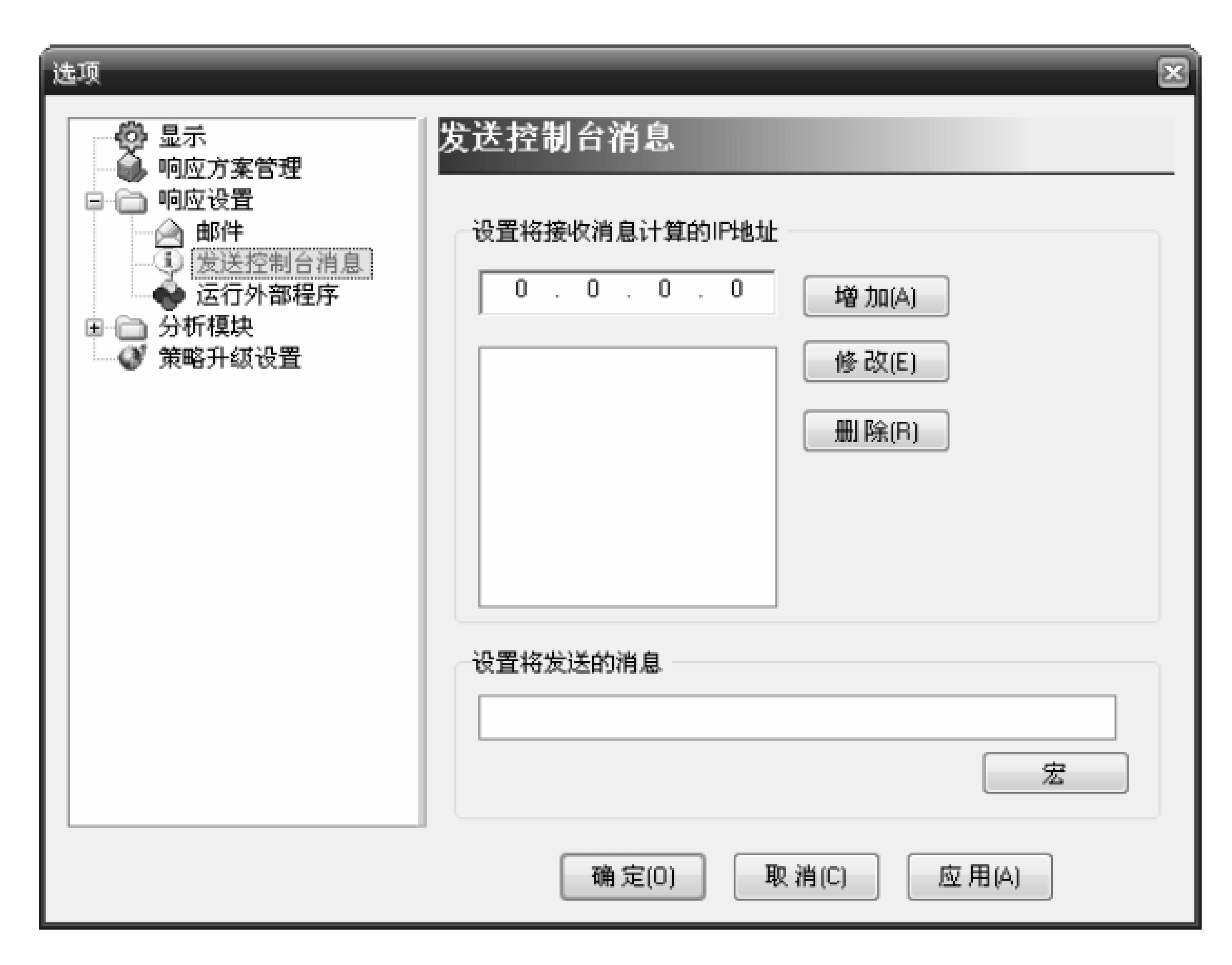


图 17-14

12 选择【响应设置】➢【运行外部程序】功能项，在其中可以对外部程序的完整路径和参数进行设置，如图 17-15 所示。



图 17-15

13 如图 17-16 所示，选择【分析模块】功能项，在其中可以对各个分析模块的参数进行个性化的设置，如是否启用该分析模块，检测的端口，日志缓冲区的大小，是否保存日志等。



图 17-16

14 选择【策略升级设置】功能项，在其中可以通过定时和手工两种方式检测策略知识库更新 Sax 入侵检测系统，并自动完整对本地知识库的更新。如果选择自动更新还必须设置更新的日期和时间，如图 17-17 所示。

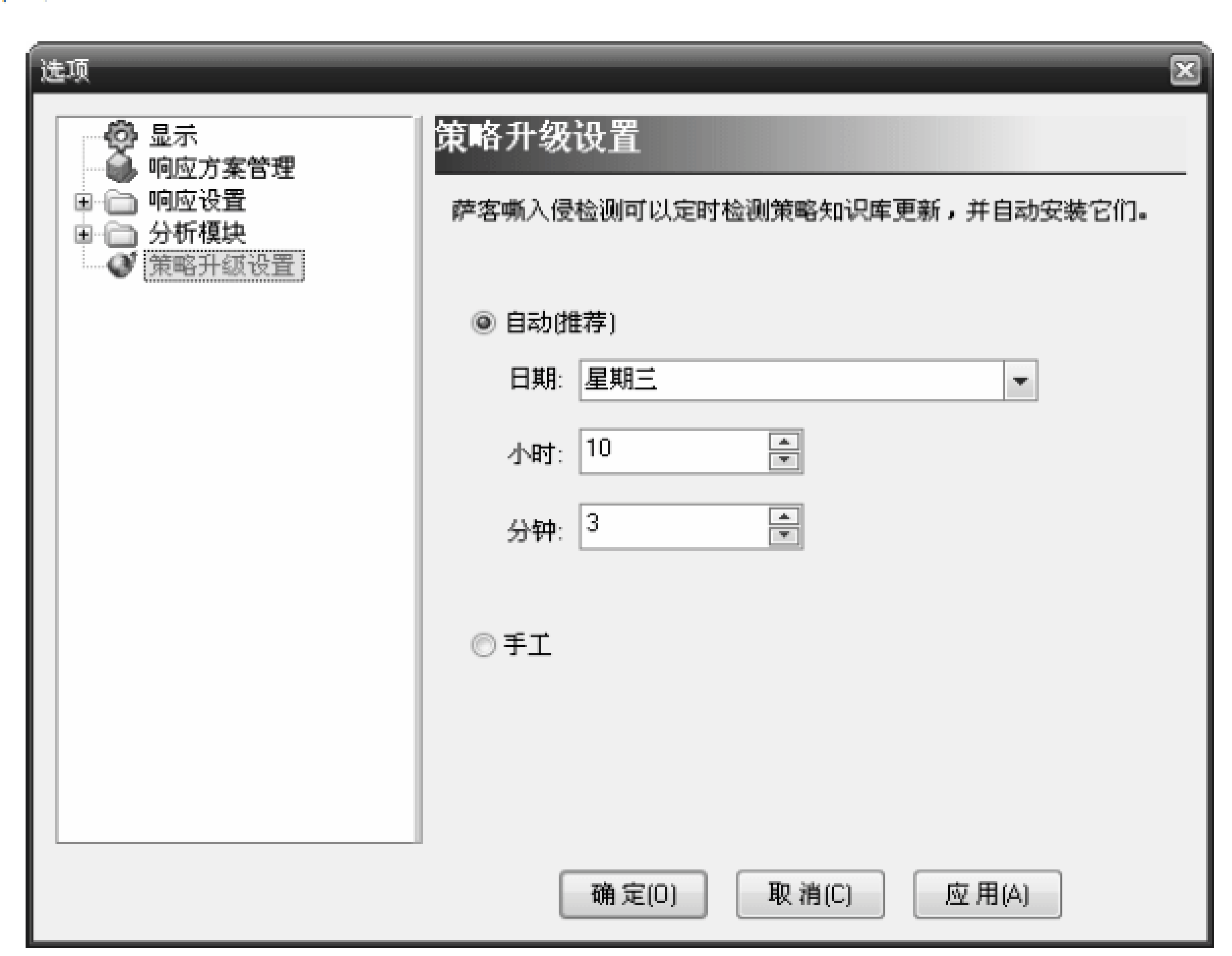


图 17-17

15 在所有选项设置完成后，单击【确定】按钮，保存设置。

2．使用 Sax 入侵检测系统

在对 Sax 入侵检测系统相关功能设置完成后，即可使用该软件来防护网络或本机系统安全了。具体的使用步骤如下。

01 在 Sax 入侵检测系统主窗口中，如图 17-18 所示，单击【开始】按钮或选择【监控】➢【开始】菜单命令，在其中可以对本机所在的局域网中的所有主机进行监控，在扫描结果中可对检测到的主机的 IP 地址、对应的 MAC 地址、本机的运行状态以及数据包统计、TCP 连接情况、FTP 分析等信息进行查看。



图 17-18

02 选择【会话】选项卡，可以看到在监控的同时，进行会话的的源 IP 地址、源端口、目标 IP 地址、目标端口、使用到的协议类型、状态、事件、数据包、字节等信息，如图 17-19 所示。

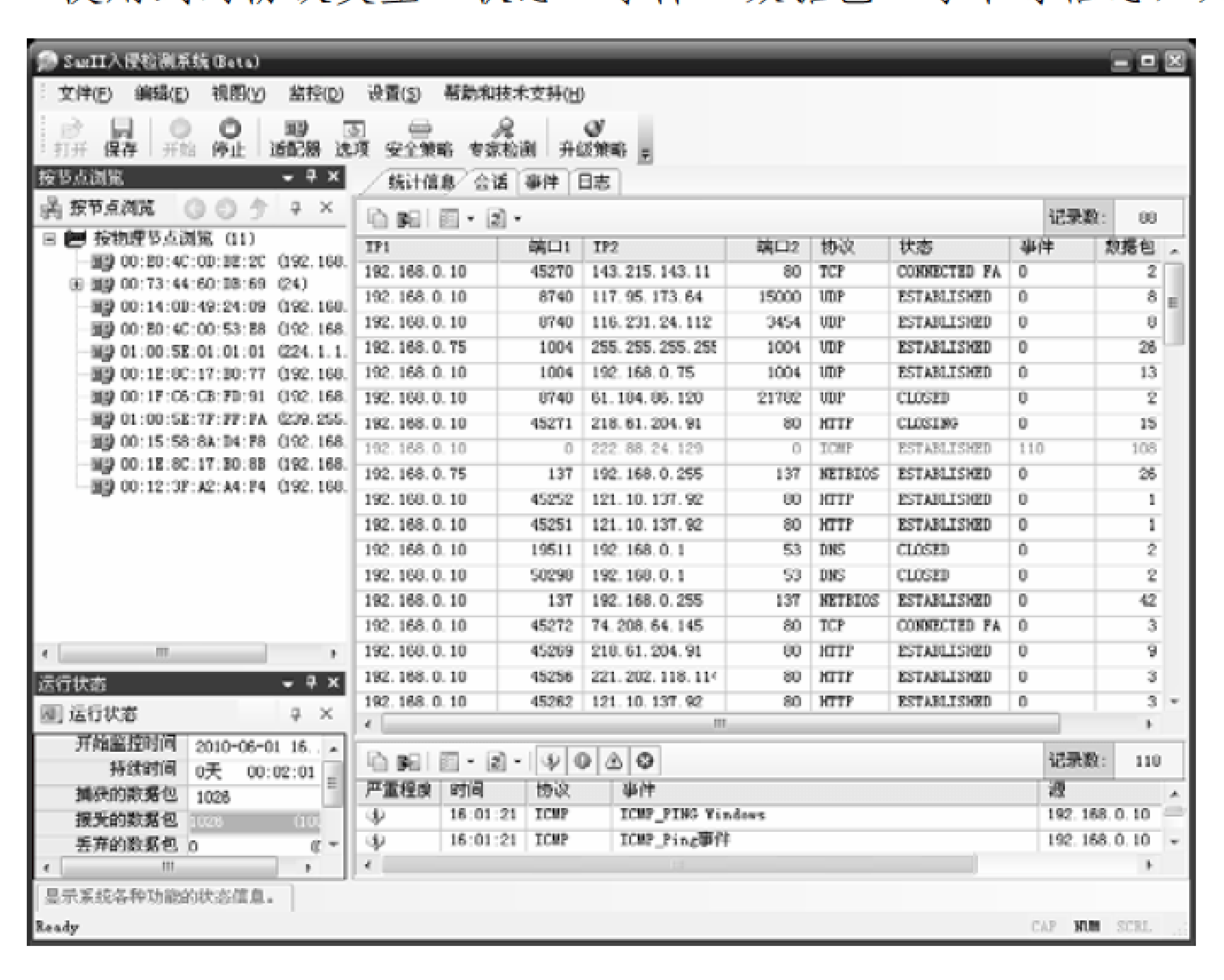


图 17-19

03 如果想分类查看会话信息，则在【会话信息】列表中右击某条信息，在弹出的快捷菜单中选择【按目标节点进行过滤】选项，以按照某个目标 IP 地址来显示会话信息，如图 17-20 所示。



图 17-20

04 如图 17-21 所示，选择【事件】选项卡，在该选项卡中可以对分类统计的各种入侵事件次数、采用日志详细记录的入侵时间、发起入侵的计算机、严重程度、采用的方式等信息进行查看。

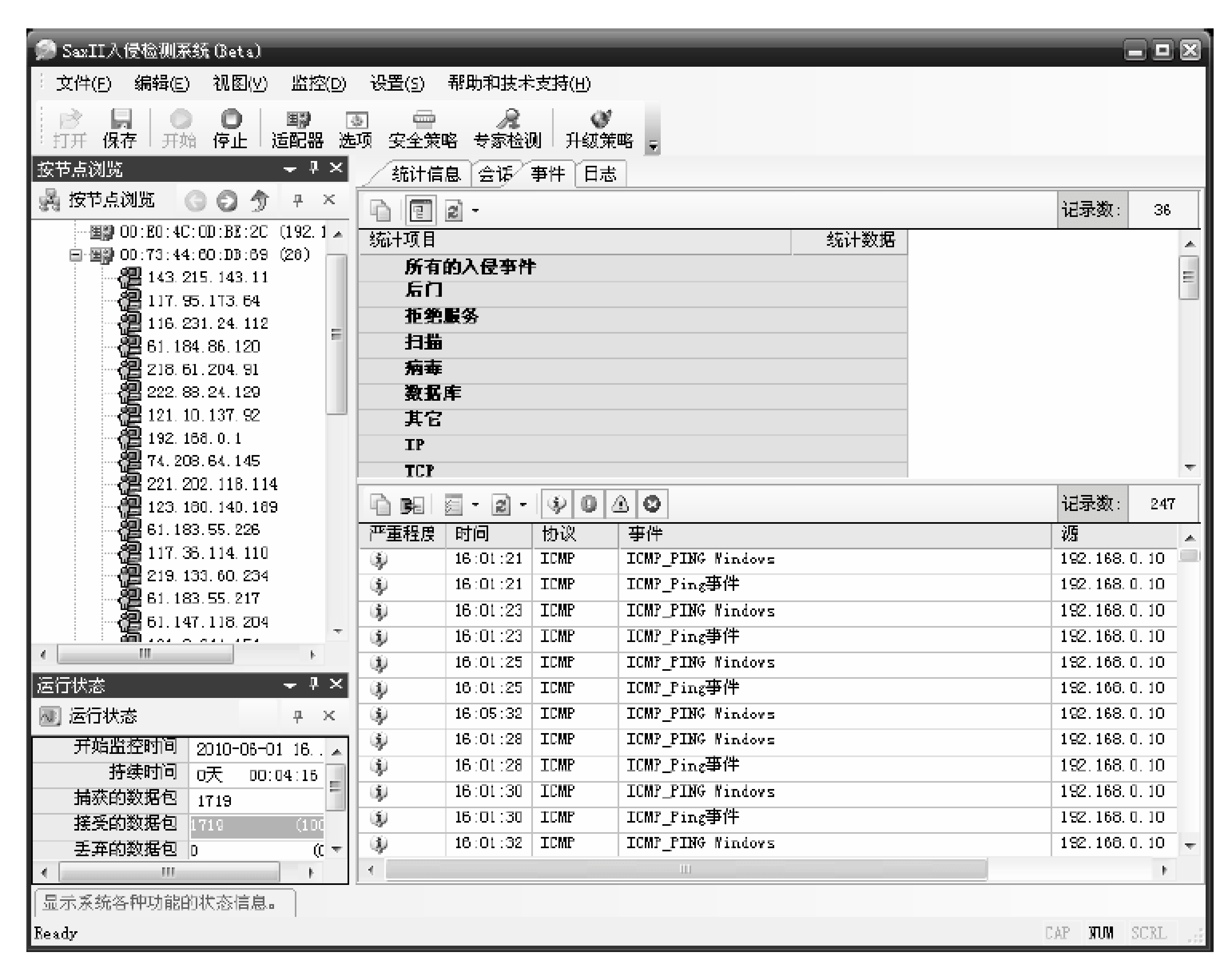


图 17-21

05 如图 17-22 所示，选择【日志】选项卡，在其中记录了 HTTP 请求、收发邮件信息、FTP 传输、MSN 和 QQ 通讯等相关信息，除了可以对这些信息进行查看外，还可以将其保存为日志文件。

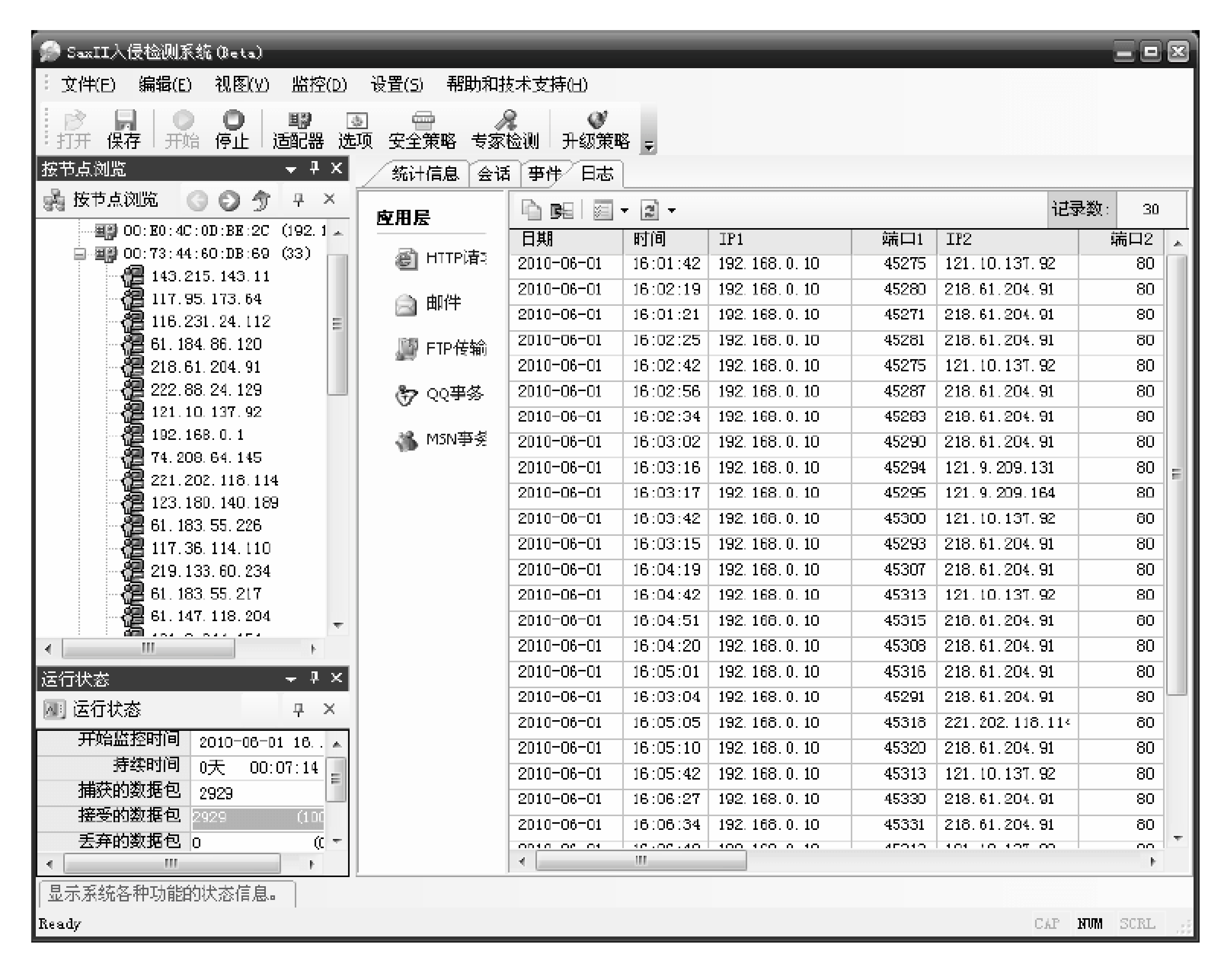


图 17-22

06 在【日志】选项卡下可自行定义日志的显示格式，单击【自定义列】按钮（如图 17-22 所示），在打开的快捷菜单中取消勾选相应的复选框即可，如图 17-23 所示。



图 17-23

07 如图 17-22 所示，在左边的节点列表中右击某个物理地址，在弹出的快捷菜单中选择【增加别名】选项，打开【增加别名】对话框，如图 17-24 所示。

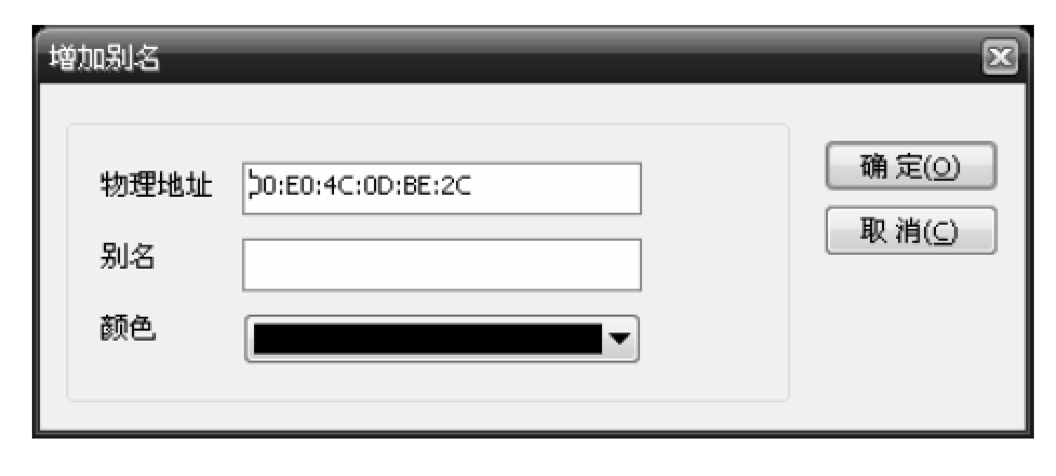


图 17-24

08 在图 17-24 所示【别名】文本框中输入名称，然后单击【确定】按钮，使该物理地址显

示刚自定义的名称，如图 17-25 所示。

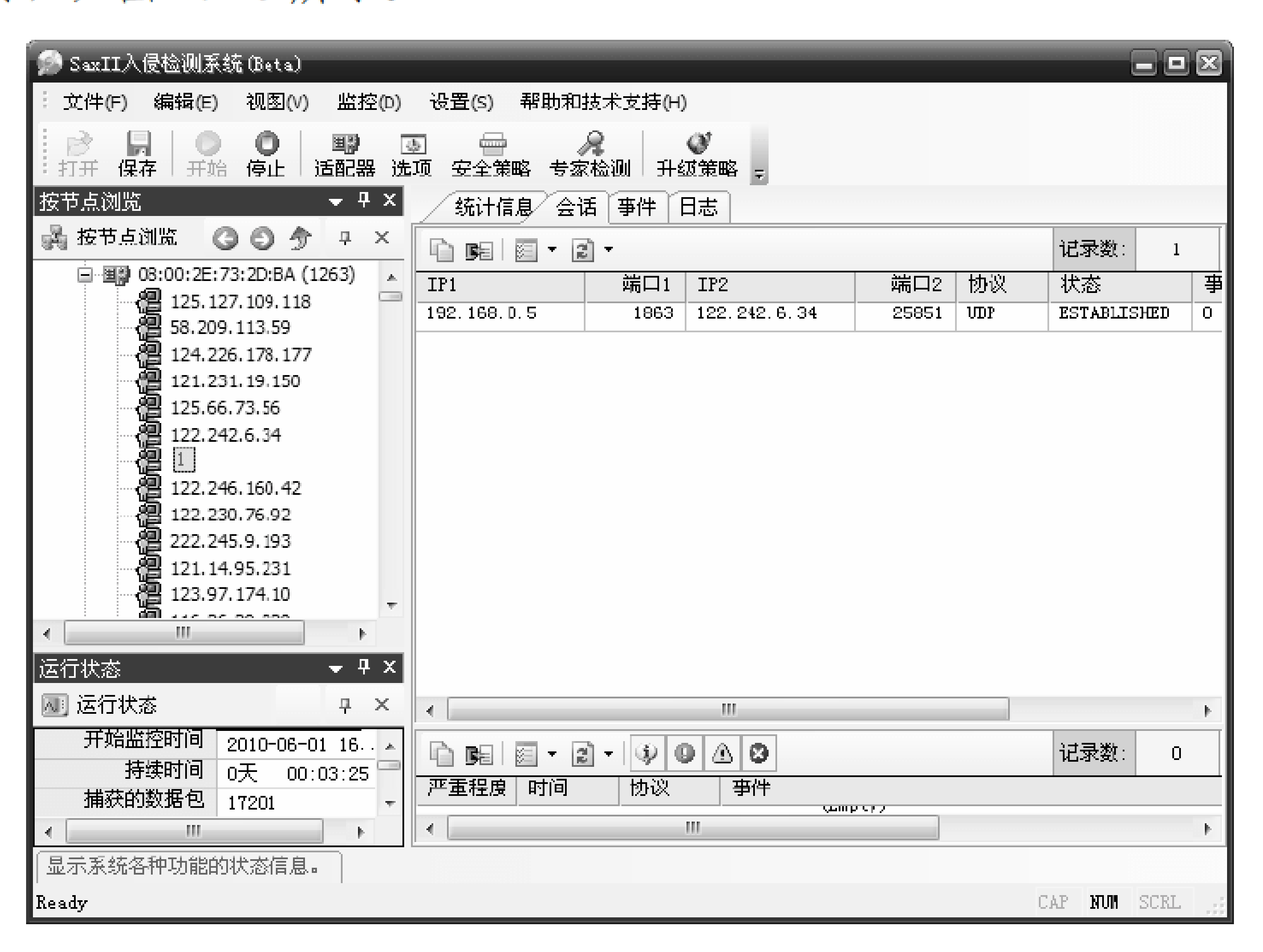


图 17-25

09 用户在遇到不能解决的问题时，可选择【帮助和技术支持】➢【帮助主题】菜单命令，在打开的【帮助】窗口中查找所需要的问题解答，如图 17-26 所示。

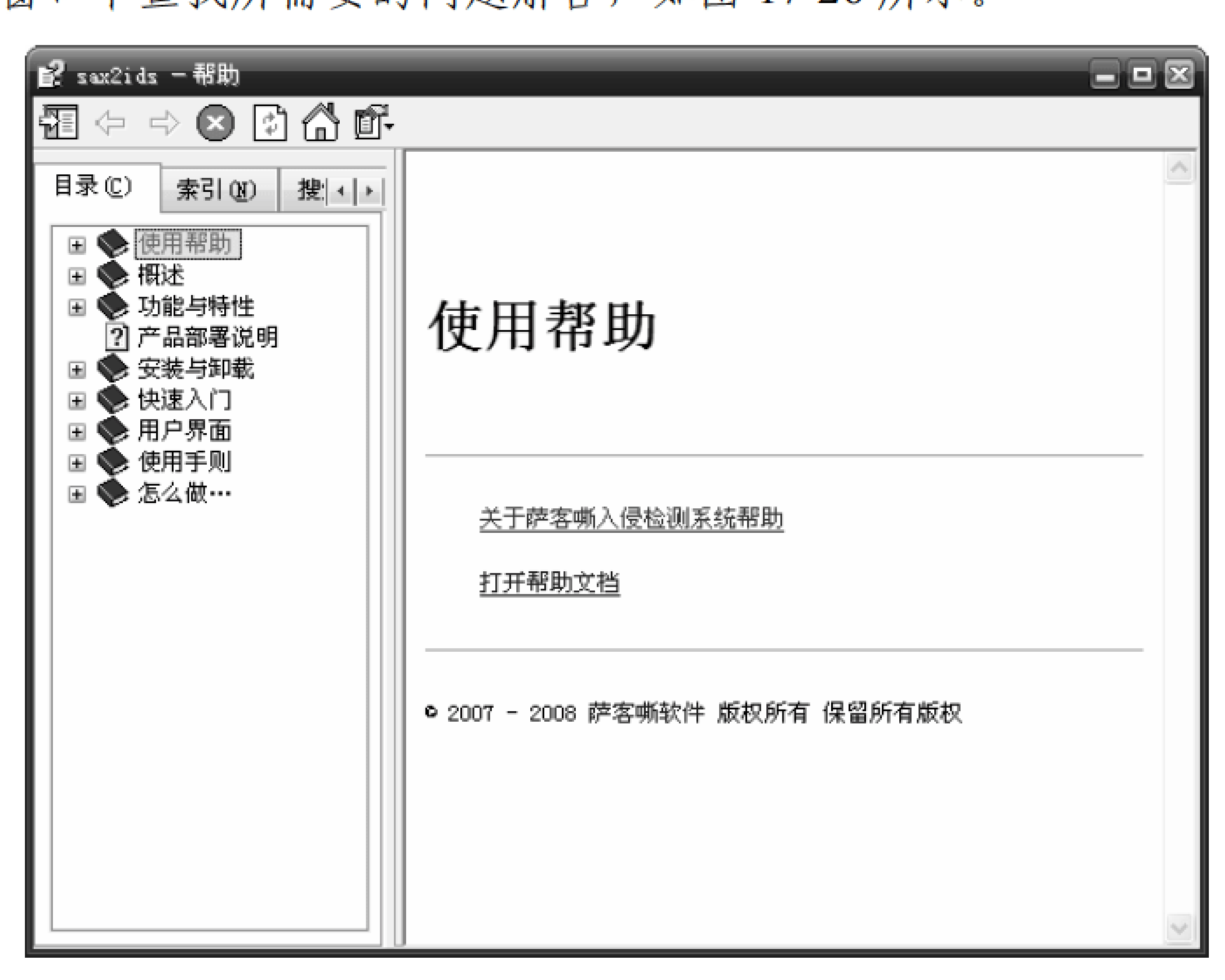


图 17-26

17.3.3 使用 BlackICE 入侵检测系统

BlackICE Server Protection 软件（简称 BlackICE）拥有强大的检测、分析以及防护功能，可以随时随地侦察出谁在扫描计算机的端口，而且简单好用。它可以在入侵者进入之前进行拦截，以保护电脑不受危害，同时，可以收集入侵者的 IP 地址、计算机名称、网络系统地址、硬件地址（MAC 地址）等，并提供一个日志文件，是一款卓越的入侵检测系统。

BlackICE 软件的安装过程比其他常用软件稍微复杂一点，在安装该软件的过程中，需要用户有一个序列号才能继续进行安装。安装入侵检测系统 BlackICE 的具体操作步骤如下。

01 下载并解压 BlackICE 程序文件夹后，双击 BlackICE 应用程序图标，弹出【欢迎 ISS BlackICE 安装】对话框，如图 17-27 所示。

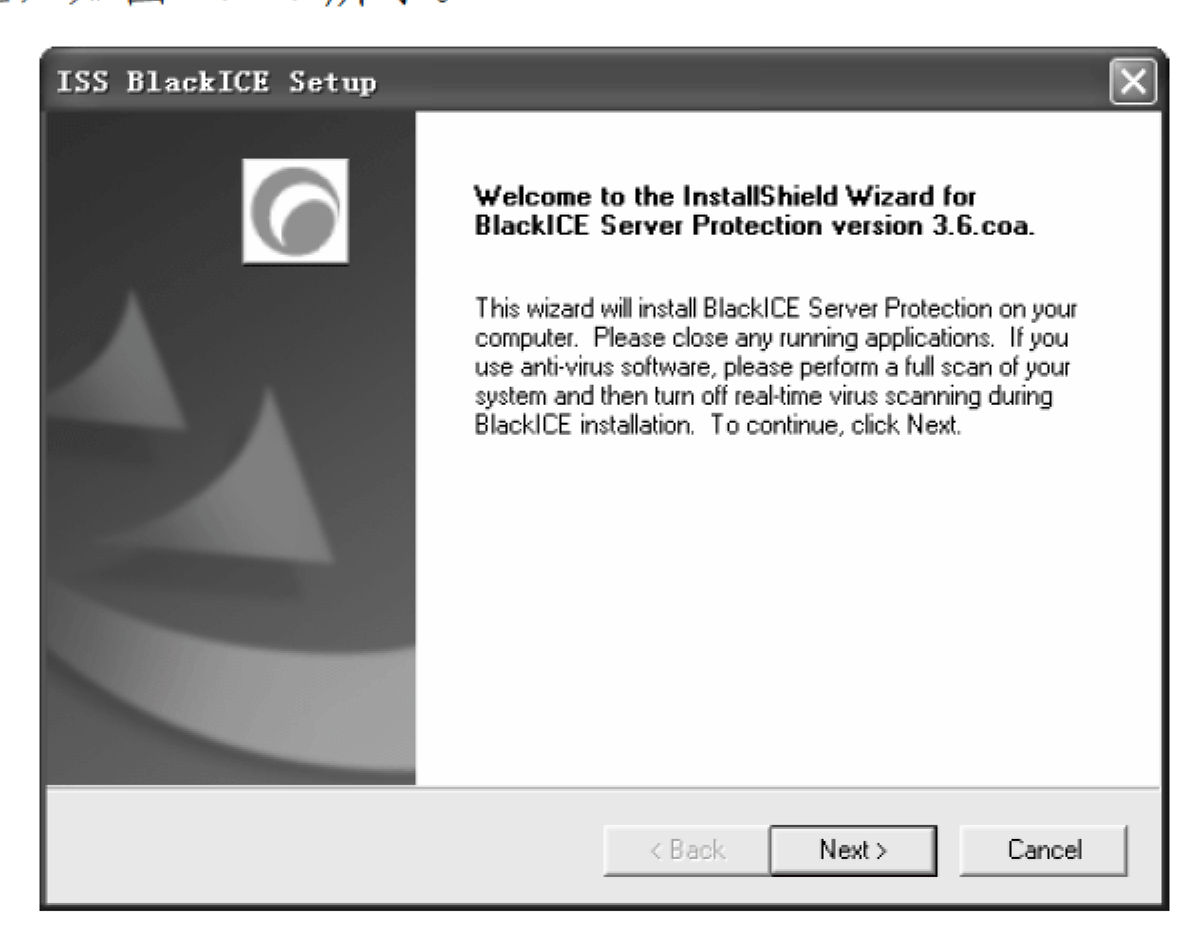


图 17-27

02 单击【Next】（下一步）按钮，打开【License Agreement】（安装许可协议）对话框，在其中可查看安装许可协议的相关内容，如图 17-28 所示。

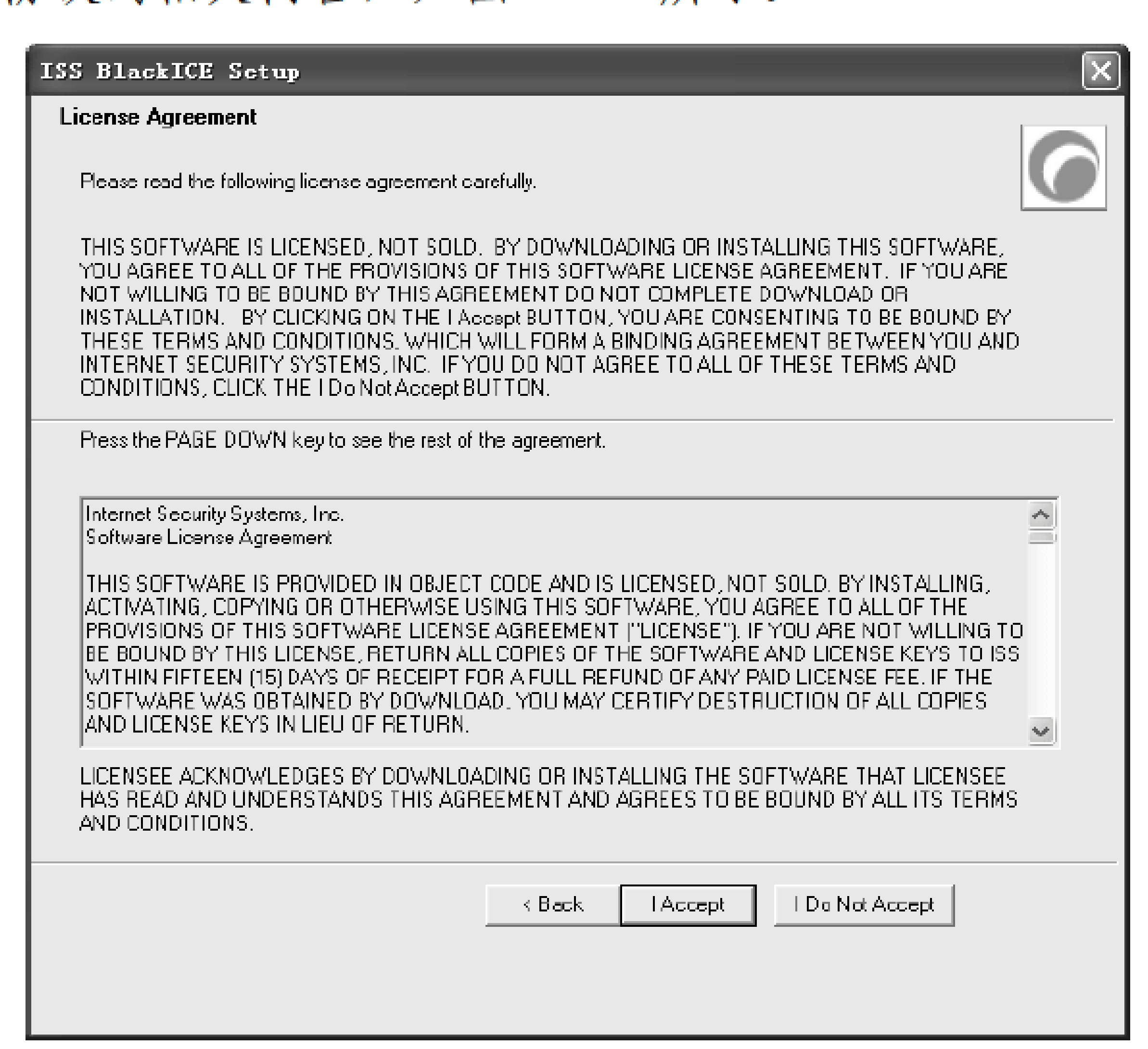


图 17-28

03 在认真阅读相关协议后，单击【I Accept】（我接受）按钮，打开【BlackICE Server Protection License】（BlackICE 服务器防护许可证）对话框，如图 17-29 所示，在【License】（许可证）文本框中输入相应版本的序列号。

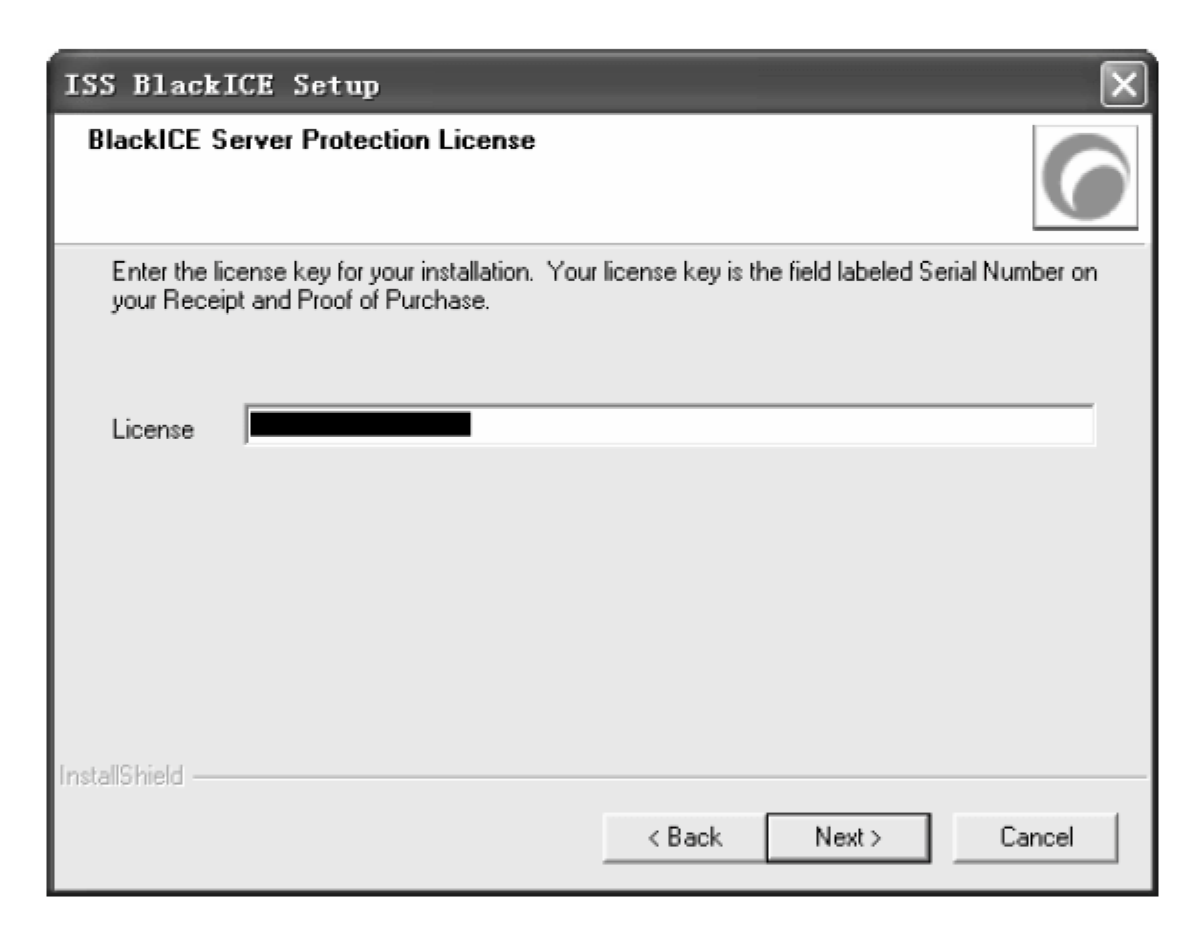


图 17-29

04 输入完成后，单击【Next】（下一步）按钮，打开【Choose Destination Location】（选择目的地位置）对话框，在其中用户可通过单击【Browse】（浏览）按钮根据实际需要更改程序安装的目标位置，如图 17-30 所示。

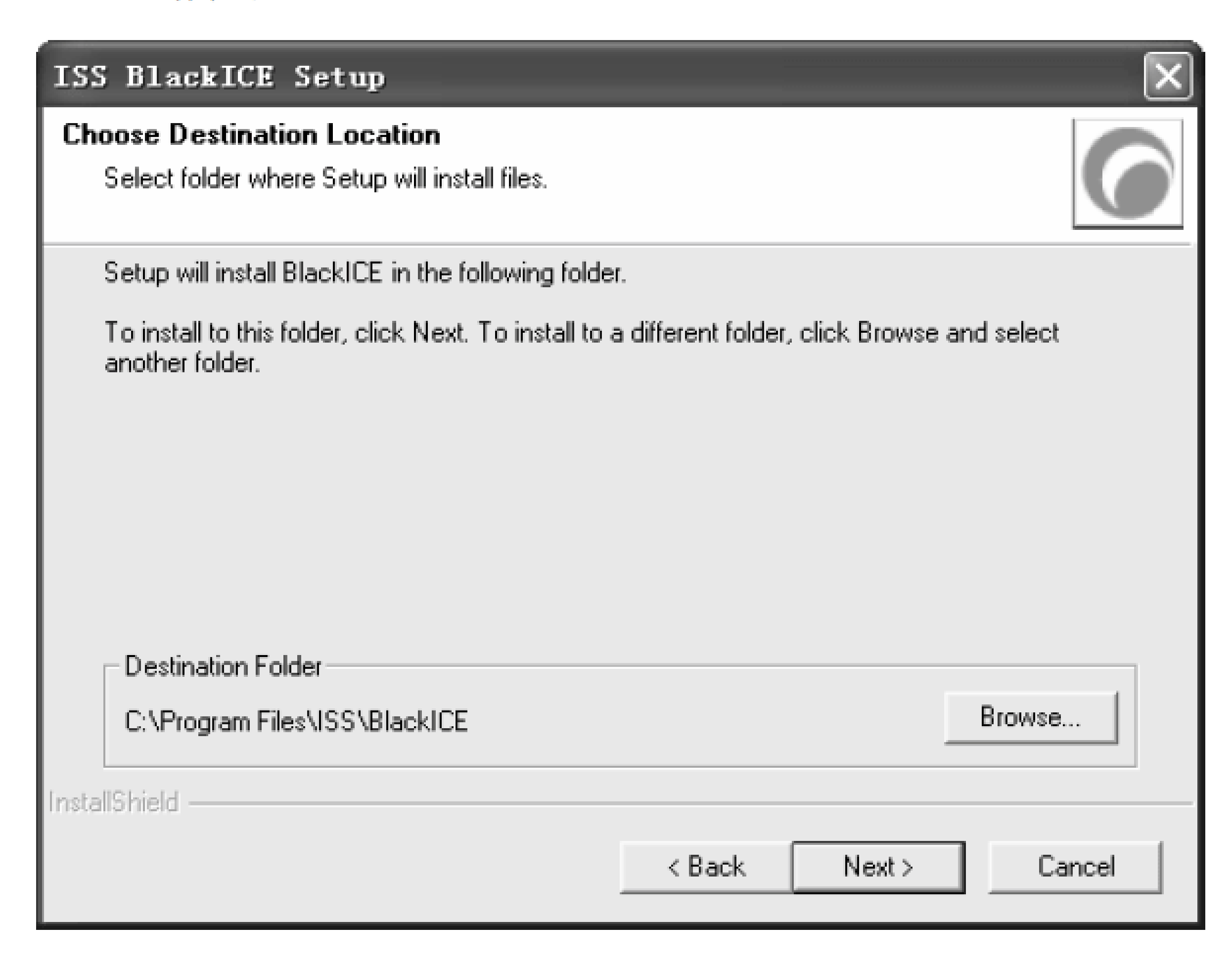


图 17-30

05 在选择好安装的目标位置后，单击【Next】（下一步）按钮，打开【Select Program Folder】（选择程序文件夹）对话框，在其中选择程序的安装文件夹，如图 17-31 所示。

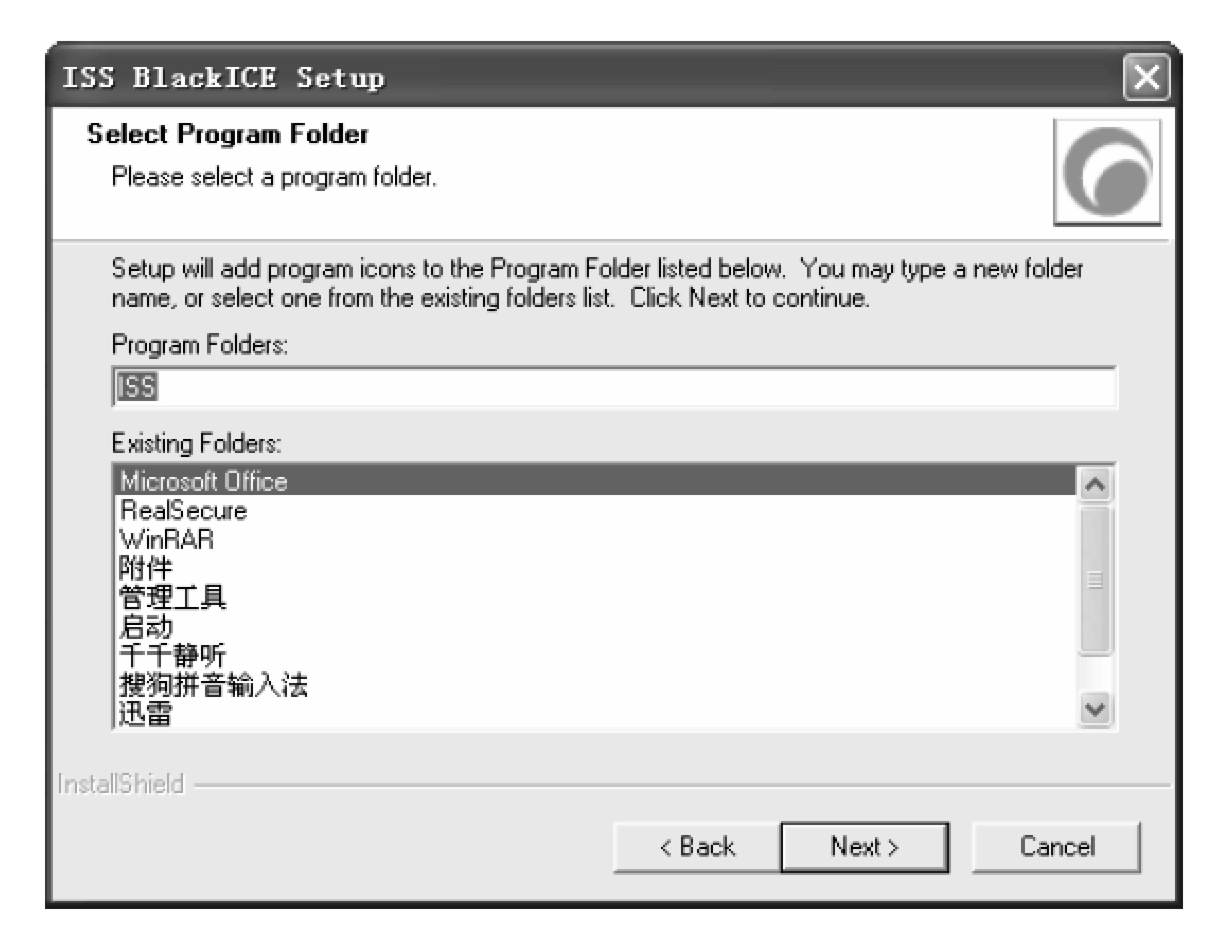


图 17-31

06 选择完毕后，单击【Next】(下一步)按钮，打开【BlackICE Server Protection Configuration（BlackICE 服务器保护配置）】对话框，如图 17-32 所示，在该对话框中用户可以根据需要开启或禁用 AP（Application Protection，程序保护），这里推荐大家选择【Off】。因为如果选择【On】，BlackICE 会在复制文件之后对本机进行扫描，并记录下所有可能访问 Internet 的程序，这一过程相当耗时。

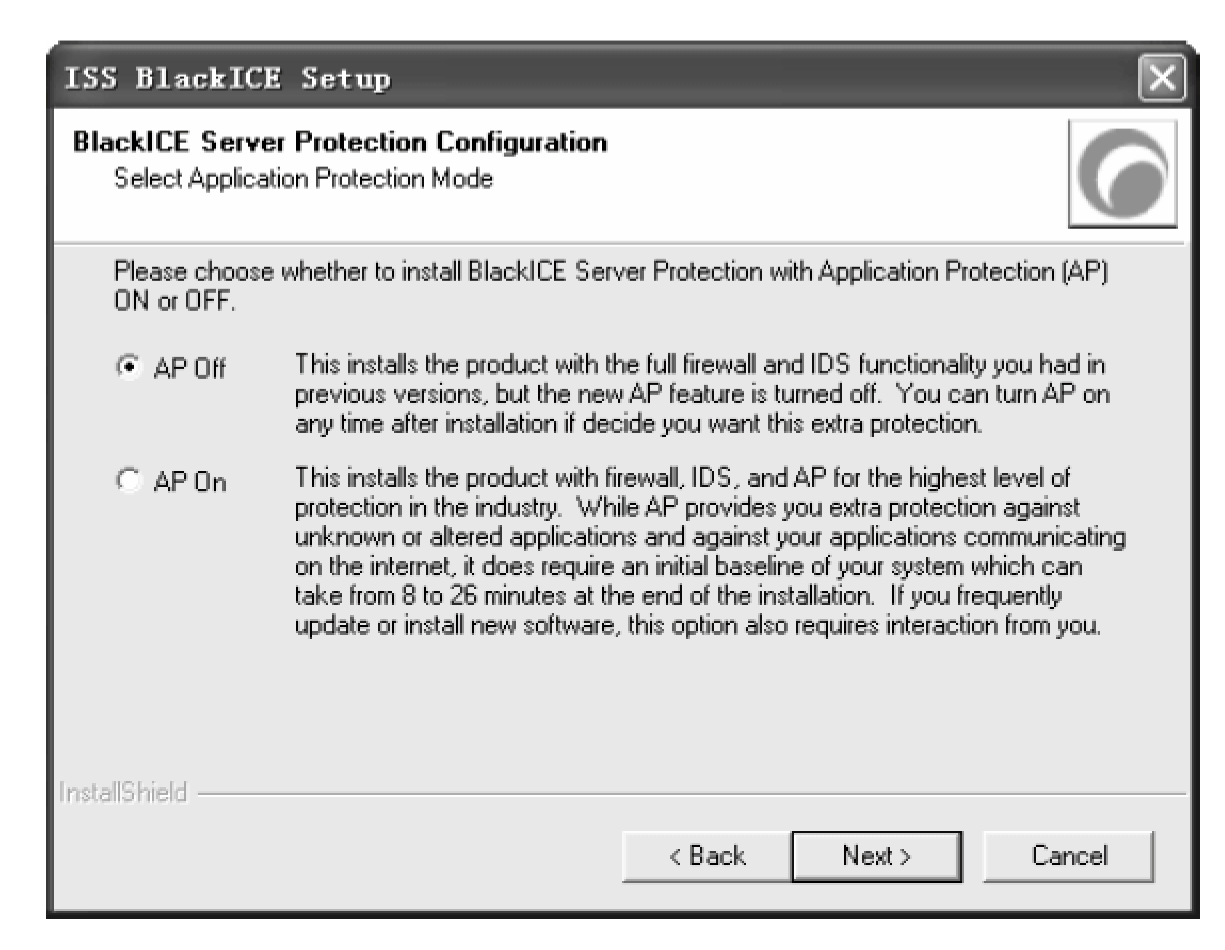


图 17-32

07 选择完毕后单击【Next】（下一步）按钮，打开【Start Copying Files】（开始复制文件）对话框，如图 17-33 所示，程序开始复制文件，并在下方的【Current Settings】（当前设置）区域中查看当前的软件的设置情况。

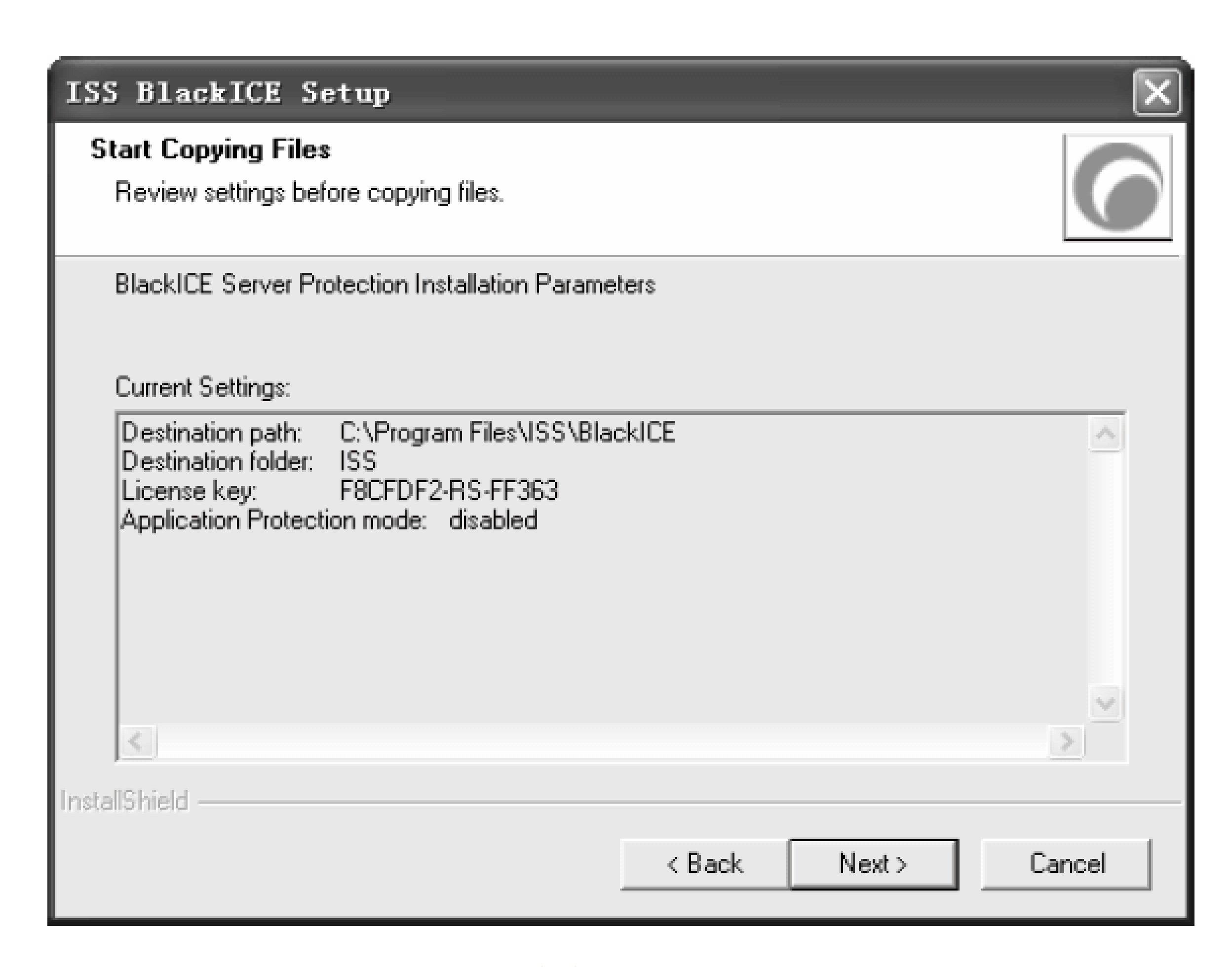


图 17-33

08 查看完毕后，单击【Next】（下一步）按钮，程序自动开始安装，并显示安装的进度条。安装完毕后，将自动弹出【InstallShield Wizard Complete】（安装向导完成）对话框，单击【Finish】（完成）按钮，结束整个安装过程，如图 17-34 所示。

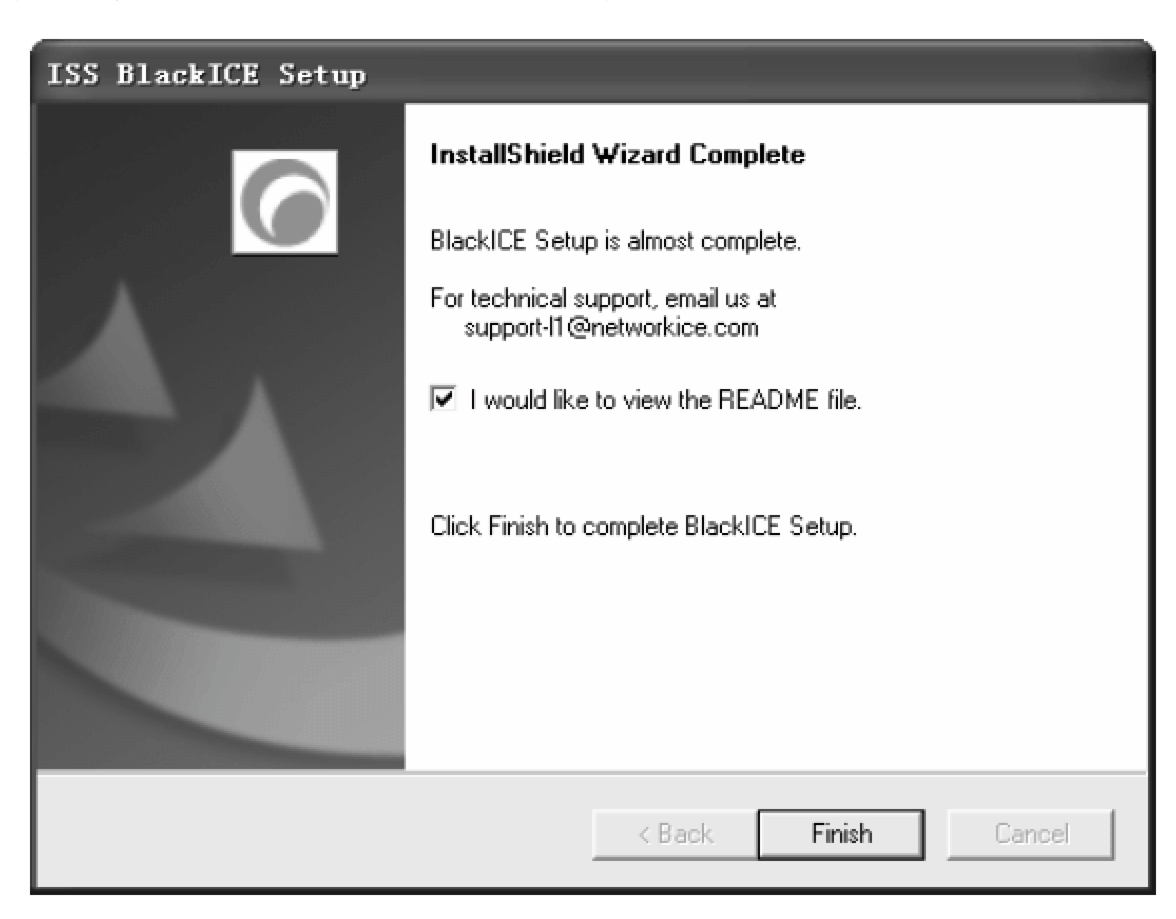


图 17-34

在安装完 BlackICE Server Protection 后，双击程序图标，即可打开 BlackICE Server Protection 操作界面，可看到该界面为英文界面。此时，用户可双击下载的汉化包对软件进行汉化处理，具体的操作步骤如下。

01 双击下载的汉化包，打开 BlackICE 汉化程序的【欢迎使用汉化包】对话框，如图 17-35 所示。

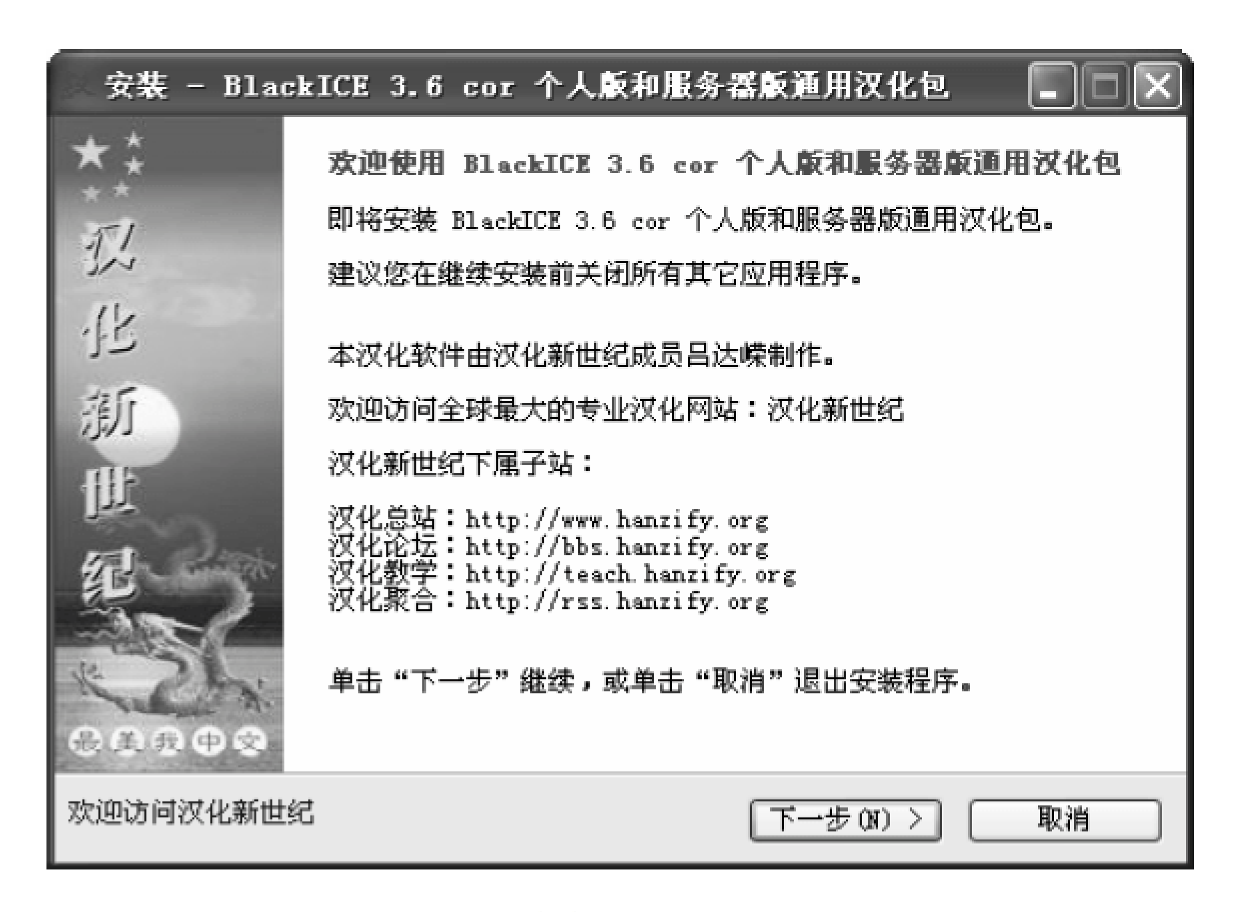


图 17-35

02 单击【下一步】按钮，打开【信息】对话框，该对话框中描述了 BlackICE 软件的概述及安装方法，如图 17-36 所示。

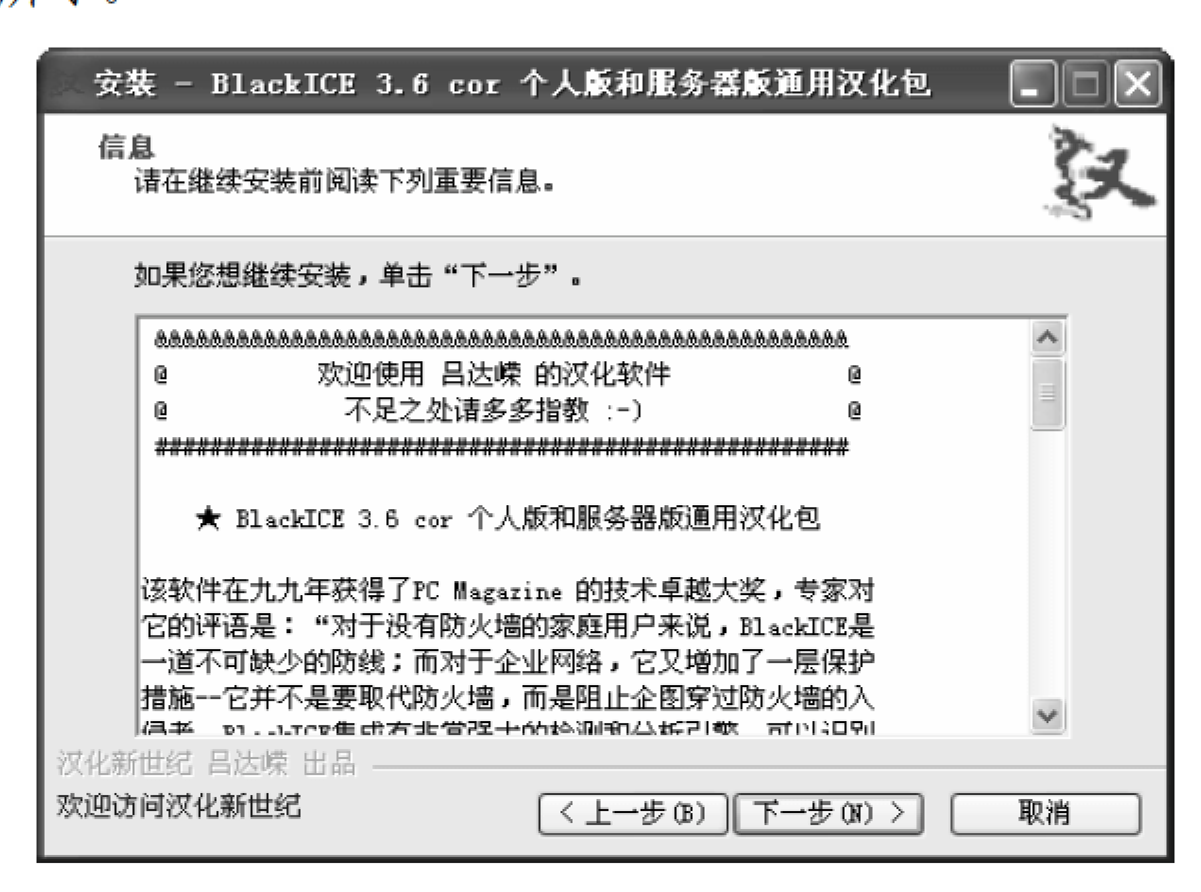


图 17-36

03 阅读完此信息后，单击【下一步】按钮，打开【选择目标位置】对话框，如图 17-37 所示。

图 17-37

04 程序默认的安装目标位置为英文原版程序的安装位置，一般没有特殊情况，不需要做出更改。单击【下一步】按钮，打开【文件夹存在】的信息提示框，提示用户文件夹已经存在，是否要安装到这个文件夹，如图 17-38 所示。

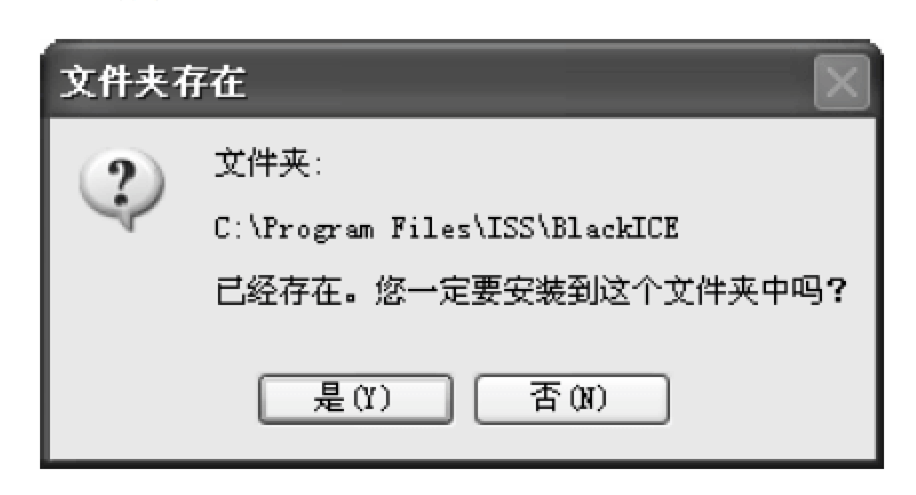


图 17-38

05 单击【是】按钮，打开【准备安装】对话框，如图 17-39 所示。

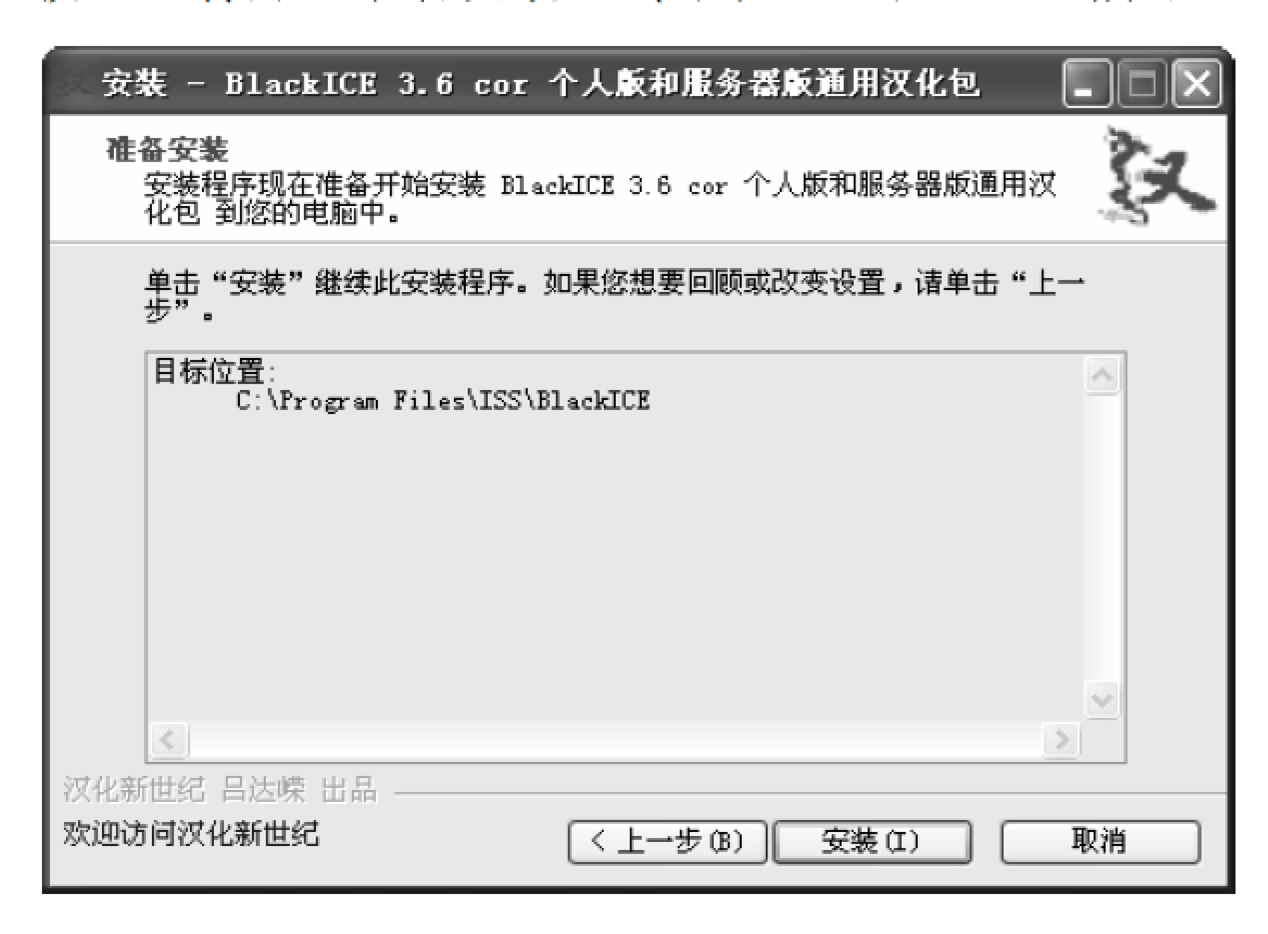


图 17-39

06 单击【安装】按钮，打开【正在安装】对话框，在其中显示了汉化补丁安装的进度，如图 17-40 所示。



图 17-40

07 稍等片刻，安装完毕后即可弹出【安装向导完成】对话框，如图 17-41 所示，在其中根

据实际需要取消勾选不必要的安装插件。

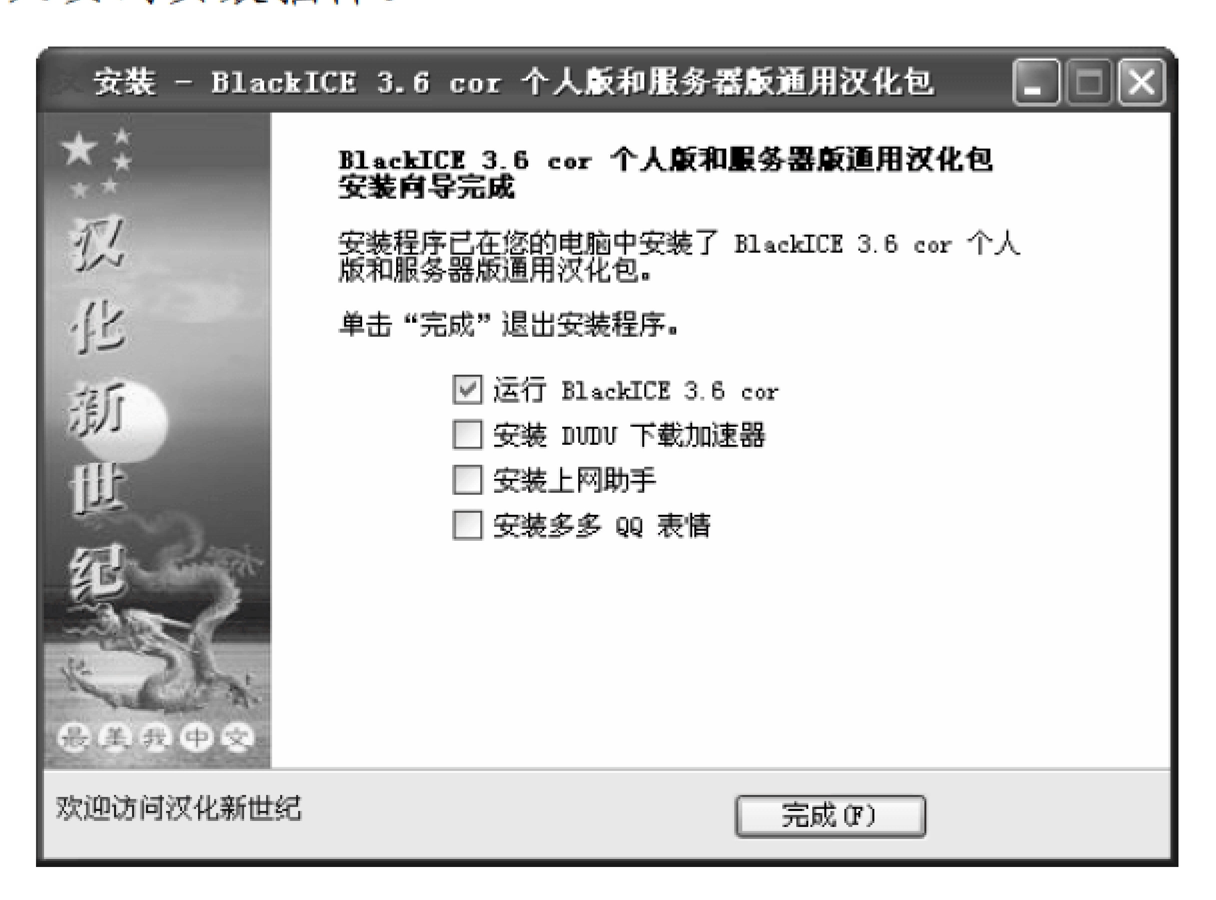


图 17-41

08 单击【完成】按钮，退出汉化补丁安装向导，并打开 BlackICE 程序主界面，可以看到已变成中文界面，如图 17-42 所示。

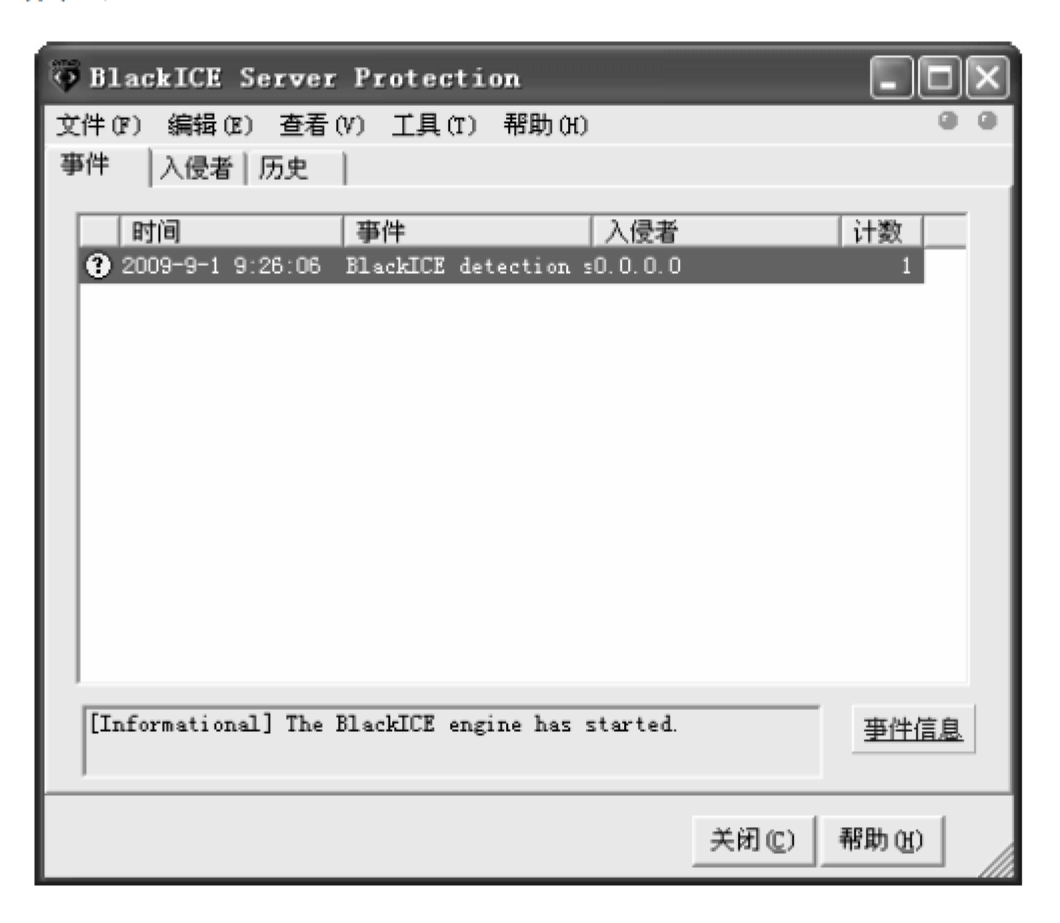


图 17-42

BlackICE 安装后即可以后台服务的方式运行，且前端系统托盘中会出现一个相应的图标，双击该图标即可打开 BlackICE 的控制台，在其中可以进行各种报警和修改程序的配置。

使用 BlackICE 入侵检测系统的操作步骤如下。

01 在图 17-42 所示的 BlackICE 主界面中，选择【工具】➢【编辑 BlackICE 设置】菜单命令，打开【BlackICE 设置】对话框，如图 17-43 所示，并切换到【防火墙】选项卡，在其中设置保护的规则和对网络文件共享能力。

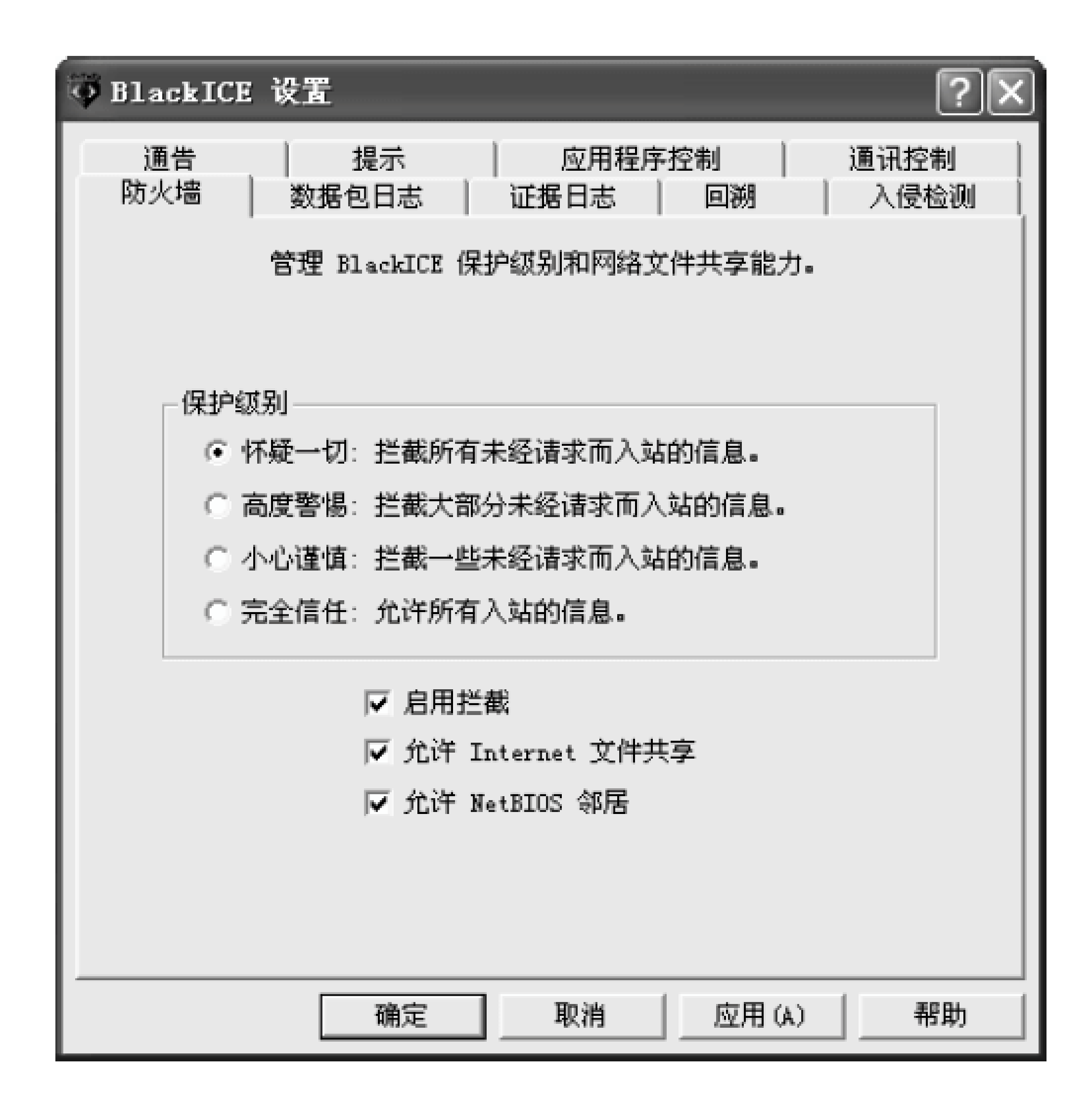


图 17-43

02 切换到【通告】选项卡，如图 17-44 所示，在该界面中的【事件通告】区域中对【可看到的指示】和【可听到的指示】进行设置，其提示信息用红、橙黄、黄和绿 4 种颜色标识，危险程度依次降低。在【更新通知】设置区域中勾选【启用检查】复选框，以设置检查更新的间隔天数。



图 17-44

03 切换到【数据包日志】选项卡，如图 17-45 所示，在该界面中勾选【启用日志】复选框，即可对所有系统信息日志文件的前缀、最大大小和文件的最大数量进行设置。

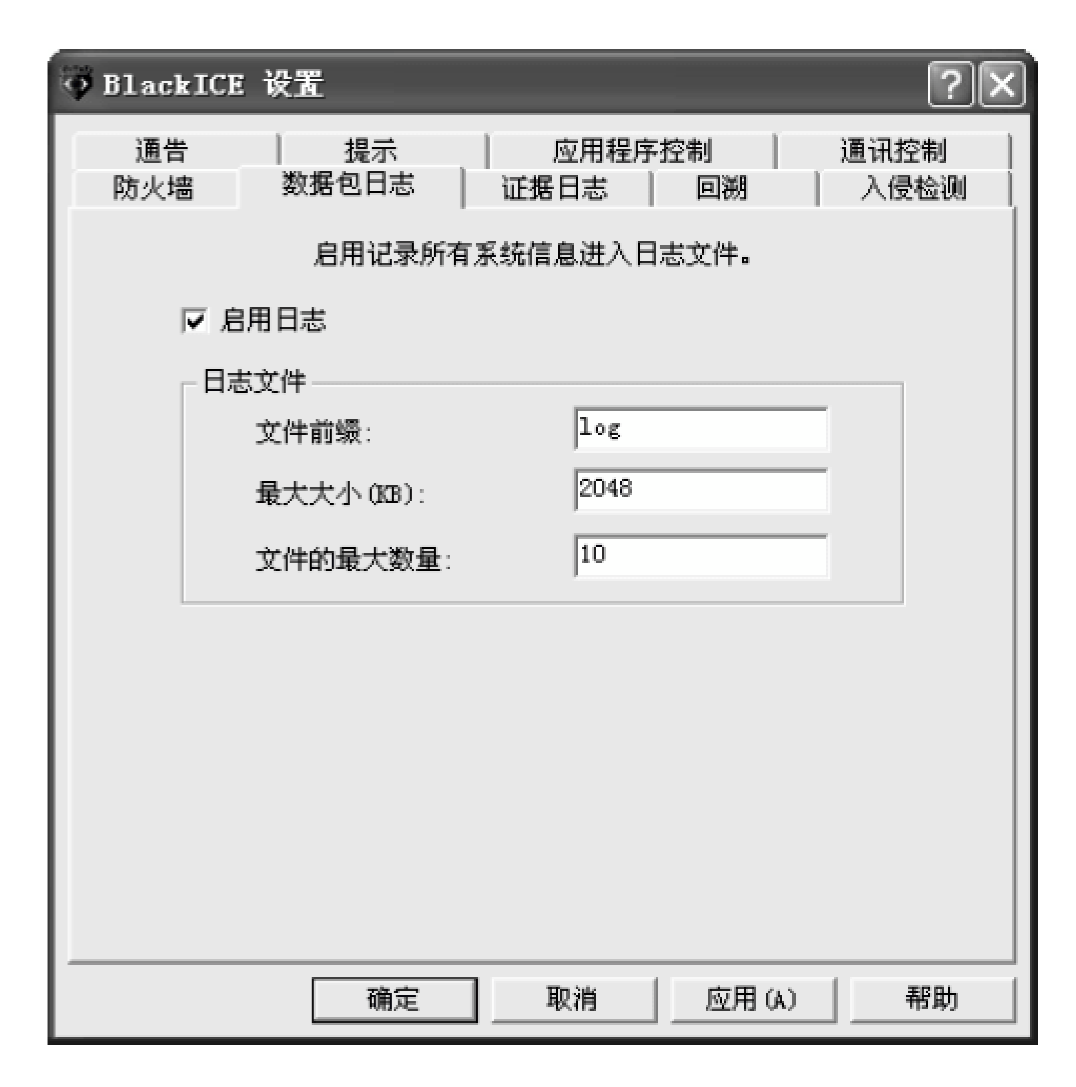


图 17-45

04 切换到【提示】选项卡，如图 17-46 所示，在该界面中通过勾选相应的复选框，对检测到可疑信息后是否显示确认对话框、显示工具提示以及当服务停止时显示提示进行设置。

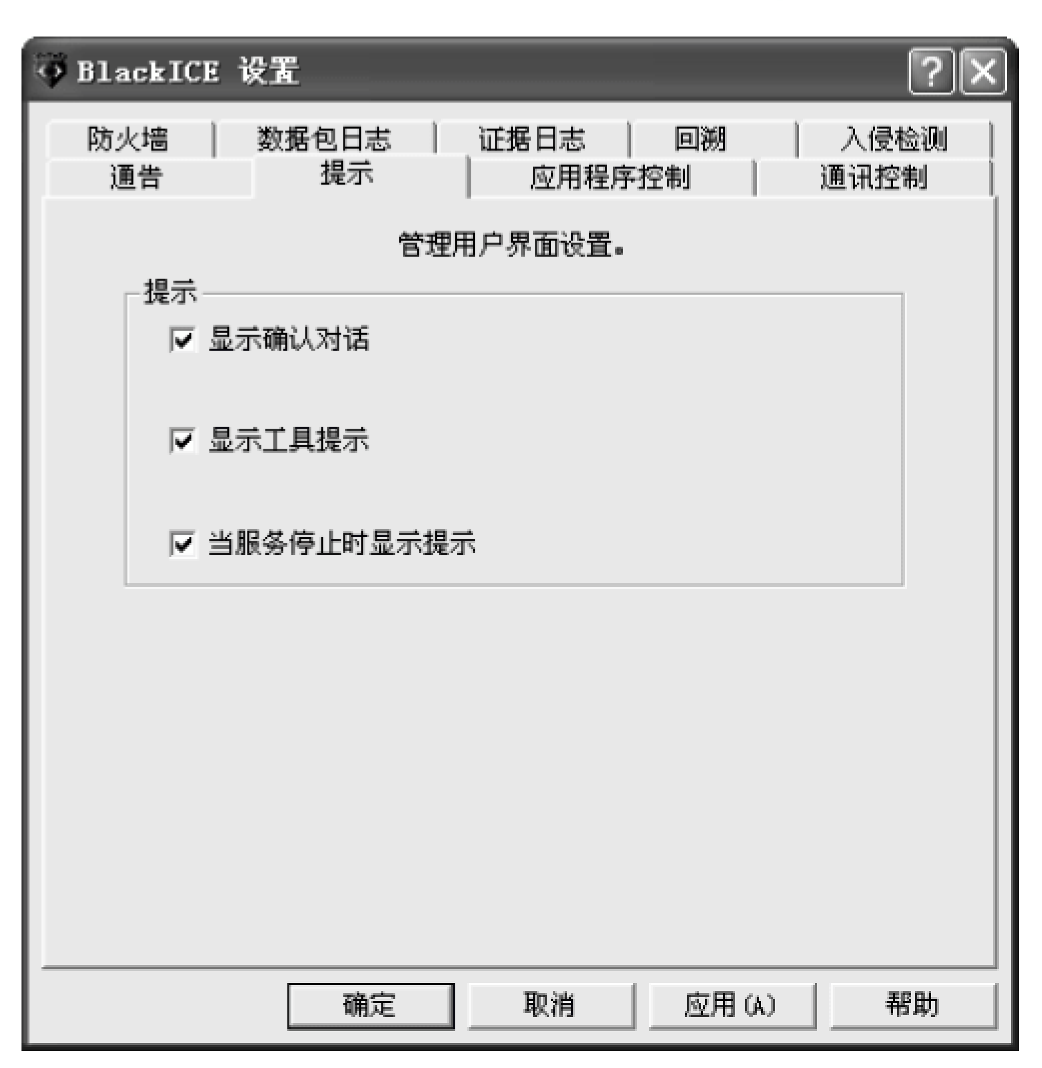


图 17-46

05 切换到【证据日志】选项卡，并勾选【启用日志】复选框，即可在其下方设置从可疑的入侵者那里收集过来的日志文件的前缀、最大大小和文件的最大数量，一般采用默认设置，如图 17-47 所示。

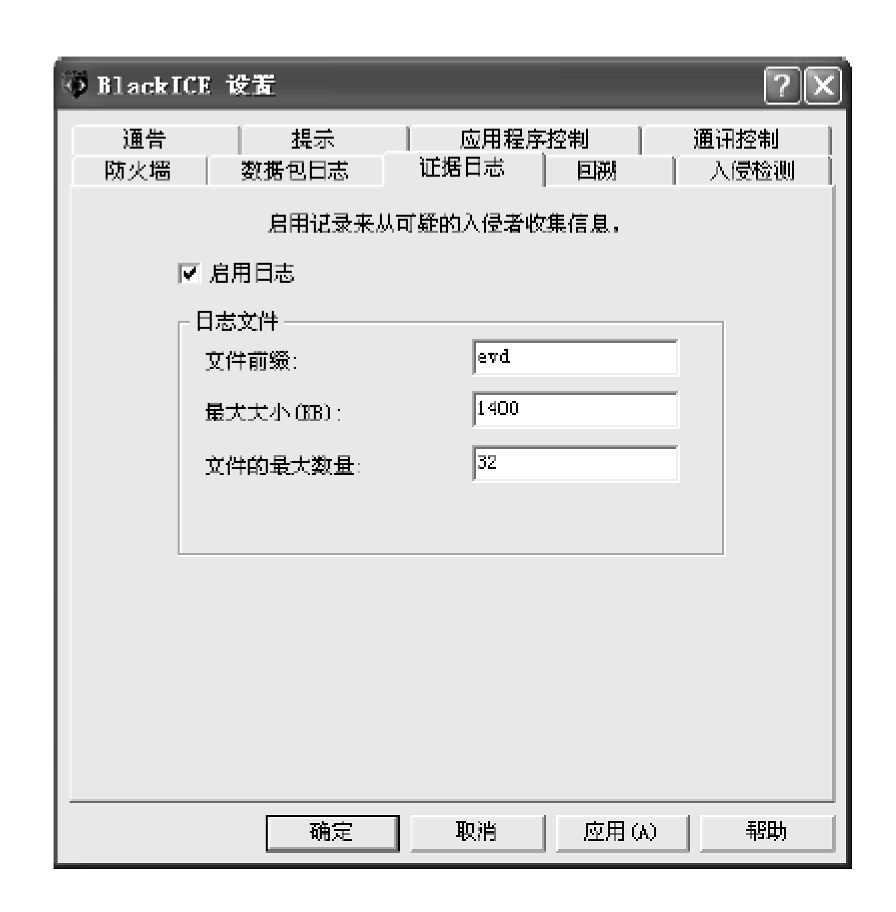


图 17-47

06 切换到【应用程序控制】选项卡，如图 17-48 所示，勾选【启用应用程序保护】复选框，即可控制运行在该计算机上的应用程序或其他进程。

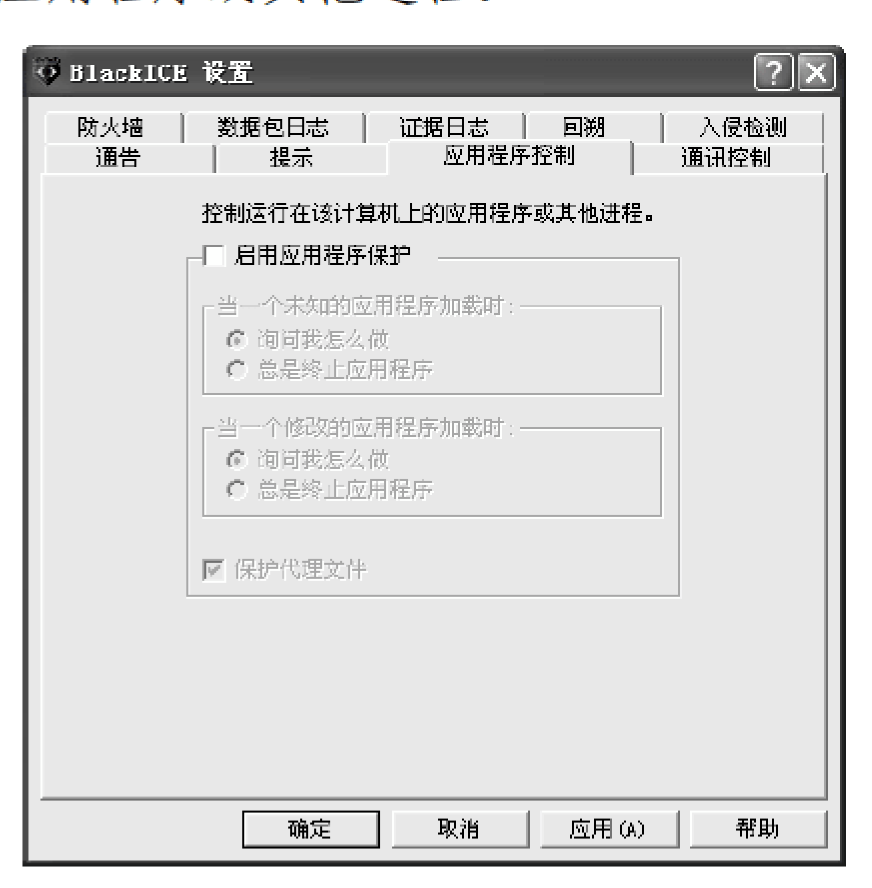


图 17-48

07 切换到【回溯】选项卡，如图 17-49 所示，在该界面中设置 BlackICE 如何以及何时定位关于入侵者的网络信息，有直接追踪和简介追踪两种方法。

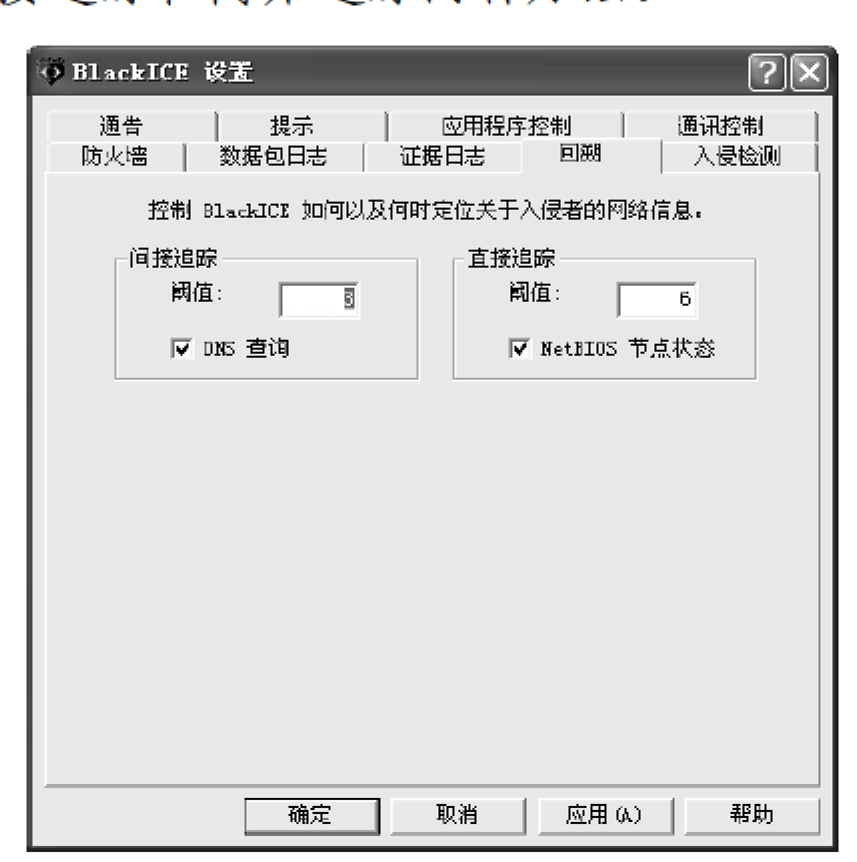


图 17-49

08 切换到【通讯控制】选项卡，如图 17-50 所示，在其中根据实际情况对来自于该计算机的网络访问进行设置。



图 17-50

09 切换到【入侵检测】选项卡，如图 17-51 所示，在该界面中查看 BlackICE 应该信任或忽略的管理地址和签名，同时通过单击【添加】按钮来添加从报告中排除要信任的地址。

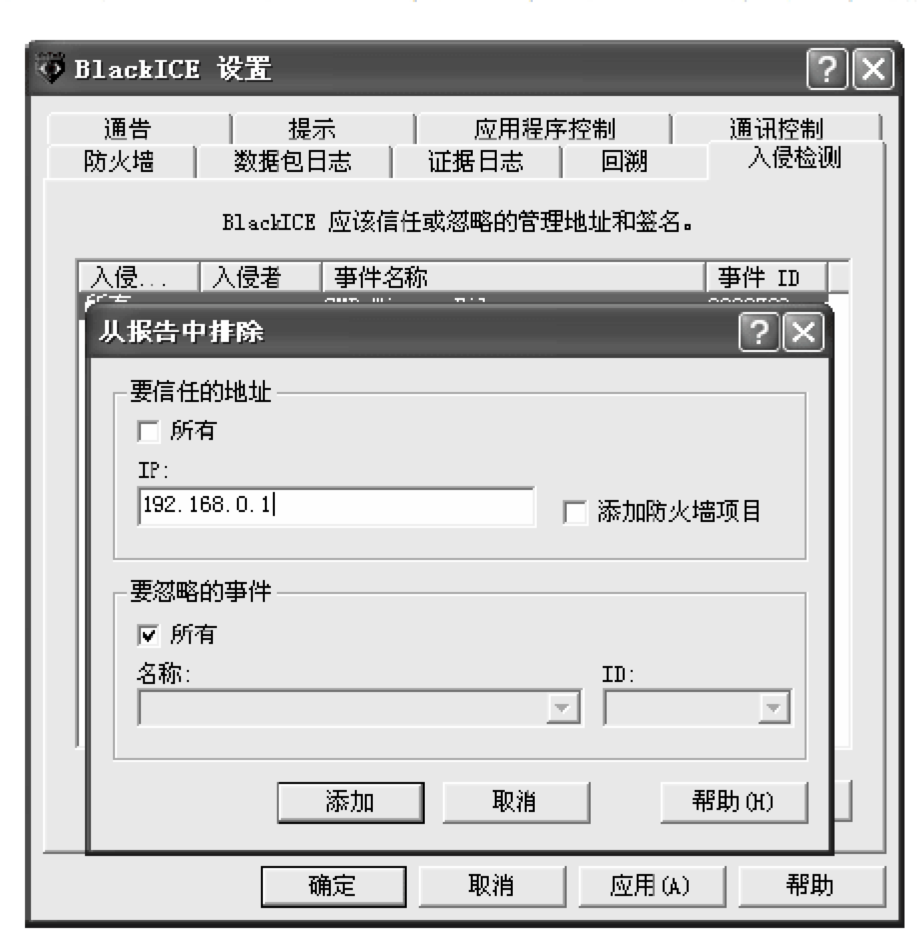


图 17-51

10 在完成上述设置后，单击【确定】按钮，在【事件】选项卡中看到入侵检测的效果即为在局域网中另一台计算机对安装了 BlackICE 的计算机进行连接时，BlackICE 立即监控到这一连接的情景。在【事件】选项卡中可看到尝试连接计算机的 IP 地址和连接方式，如图 17-52 所示。

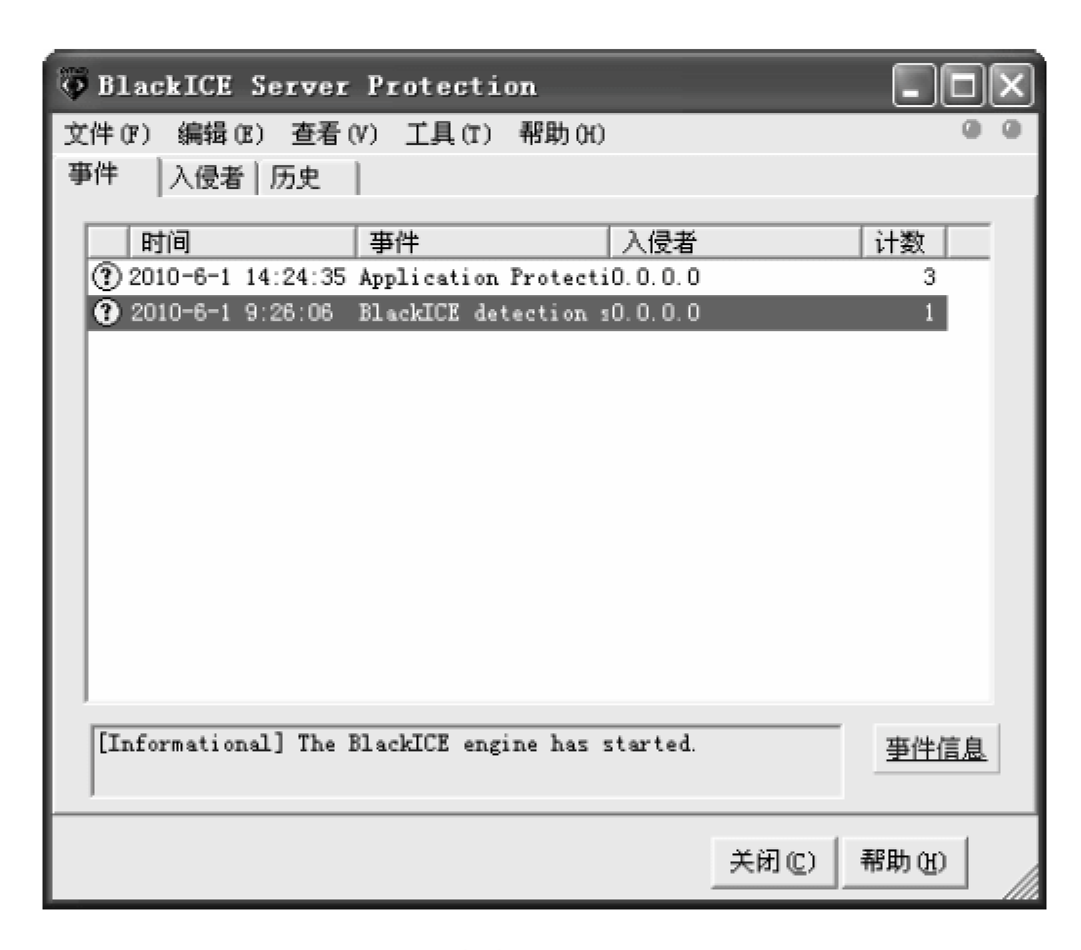


图 17-52

11 切换到【历史】选项卡中，在该界面的图标中可以看到该连接被认为是【可疑】的入侵，如图 17-53 所示。

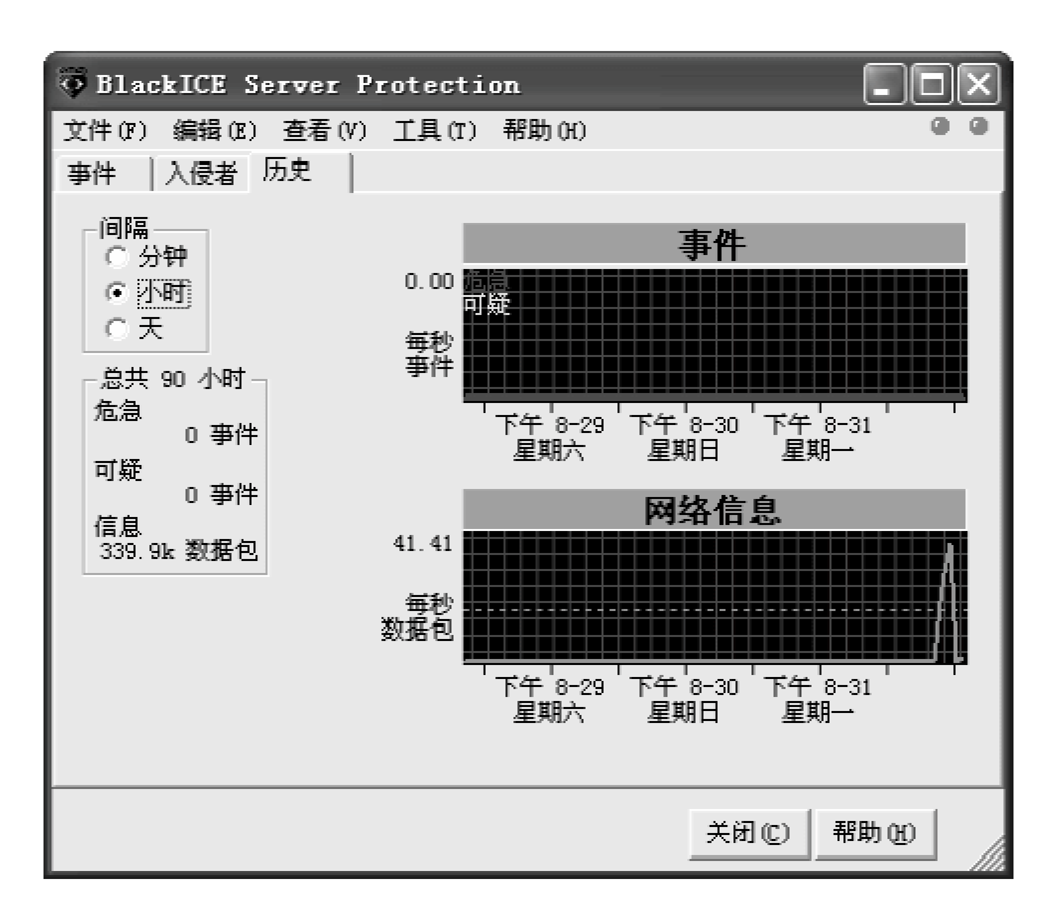


图 17-53

总之，BlackICE 在保护计算机安全方面是非常精确可靠的，不过，在使用过程中还要及时升级软件，以使软件及时增加入侵特征数据库中的特征数据，这样才能更加有效地过滤掉最新的入侵行为，从而保障计算机网络系统的安全。

17.4 项目实施 2：提高网站服务器的安全性

在了解了有关入侵检测系统的概述、分类以及常用的入侵检测系统工具外，下面再来介绍一些相关拓展内容。

17.4.1 检测网站服务器承受的压力

随着互联网的高速发展，许多企事业单位和个人都有了自己的网站和服务器。但由于资金和

技术等多方面原因，这些网站的安全性并不强。网络管理员要想保证网站服务器的安全，就必须了解如何检测网站服务器的承受压力。使用 Microsoft Web Application Stress Tool（WAS）软件可以进行实际网站压力的测试，从而找出系统潜在的问题。

1. 检测网站服务器承受的压力

在开始录制一个脚本前，需要准备好浏览器，清除浏览器中的临时文件。否则，WAS 也许不能记录所需的浏览器活动，因为浏览器可能从缓冲区而不是从所请求的服务器取得请求页面。具体的操作步骤如下。

01 首先打开 IE 浏览器，选择【工具】➢【Internet 选项】菜单命令，打开【Internet 选项】对话框，如图 17-54 所示。



图 17-54

02 切换到【常规】选项卡下，单击【删除文件】按钮，打开【是否删除 Internet 临时文件夹中的内容】提示框，如图 17-55 所示，单击【确定】按钮，即可成功删除 Internet 临时文件。



图 17-55

03 下载并安装【WAS】软件，选择【开始】➢【程序】➢【Microsoft Web Application Stress Tool】➢【Microsoft Web Application Stress Tool】菜单命令，启动 WAS 主程序。由于是第一次运行 WAS 程序，将会弹出【Create new script】（创建新的脚本）对话框，询问以何种方式创建一个新的测试脚本，显示如图 17-56 所示。



图 17-56

04 根据需要单击【Record】（记录）按钮，将会弹出【Browse Recorder—Step 1 of 2】对话框，如图 17-57 所示。



图 17-57

05 勾选所有复选框后，单击【Next】（下一步）按钮，将会弹出【Browse Recorder—Step 2 of 2】对话框，如图 17-58 所示。



图 17-58

06 单击【Finish】按钮，WAS 将启动一个浏览器窗口，在其中可以看到记录浏览器的活动情况，如图 17-59 所示。

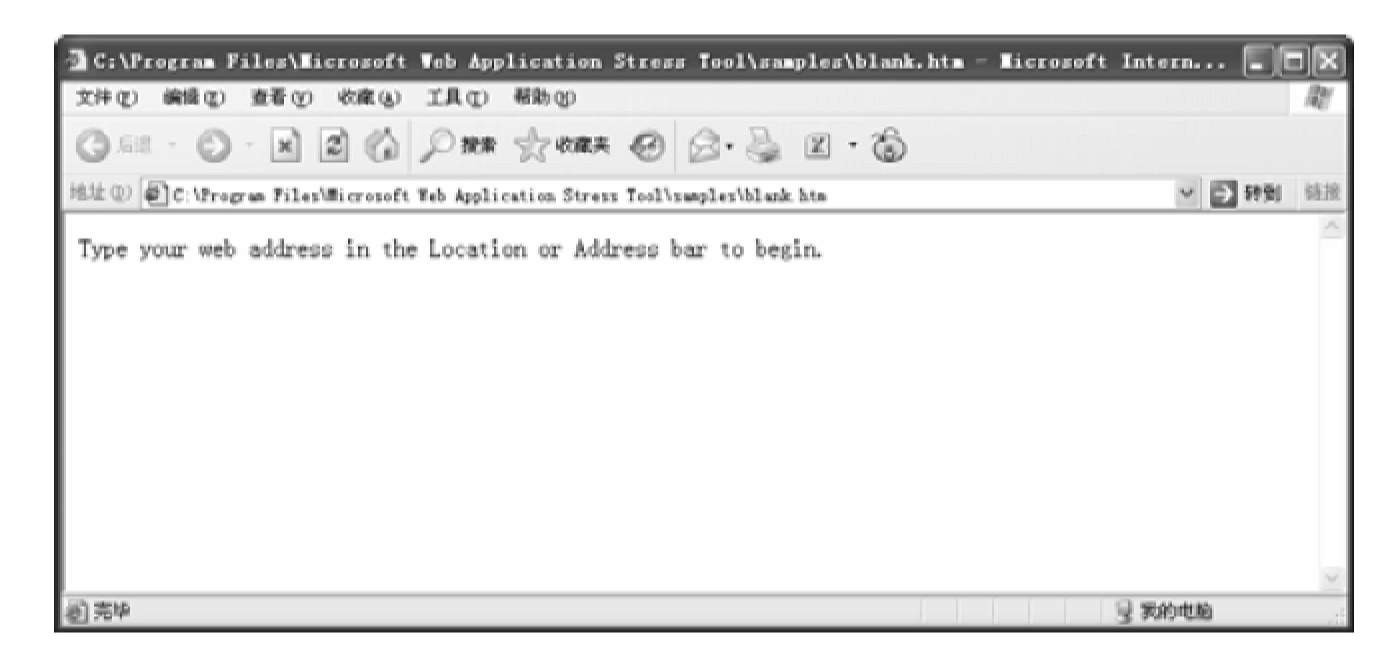


图 17-59

07 同时 WAS 会被置于记录模式，并在 IE 浏览器的地址栏里输入要测试的网站地址，按回车键后，此时在【WAS】主窗口中即可看到 HTTP 信息跟随浏览活动而进行实时更新，如图 17-60 所示。

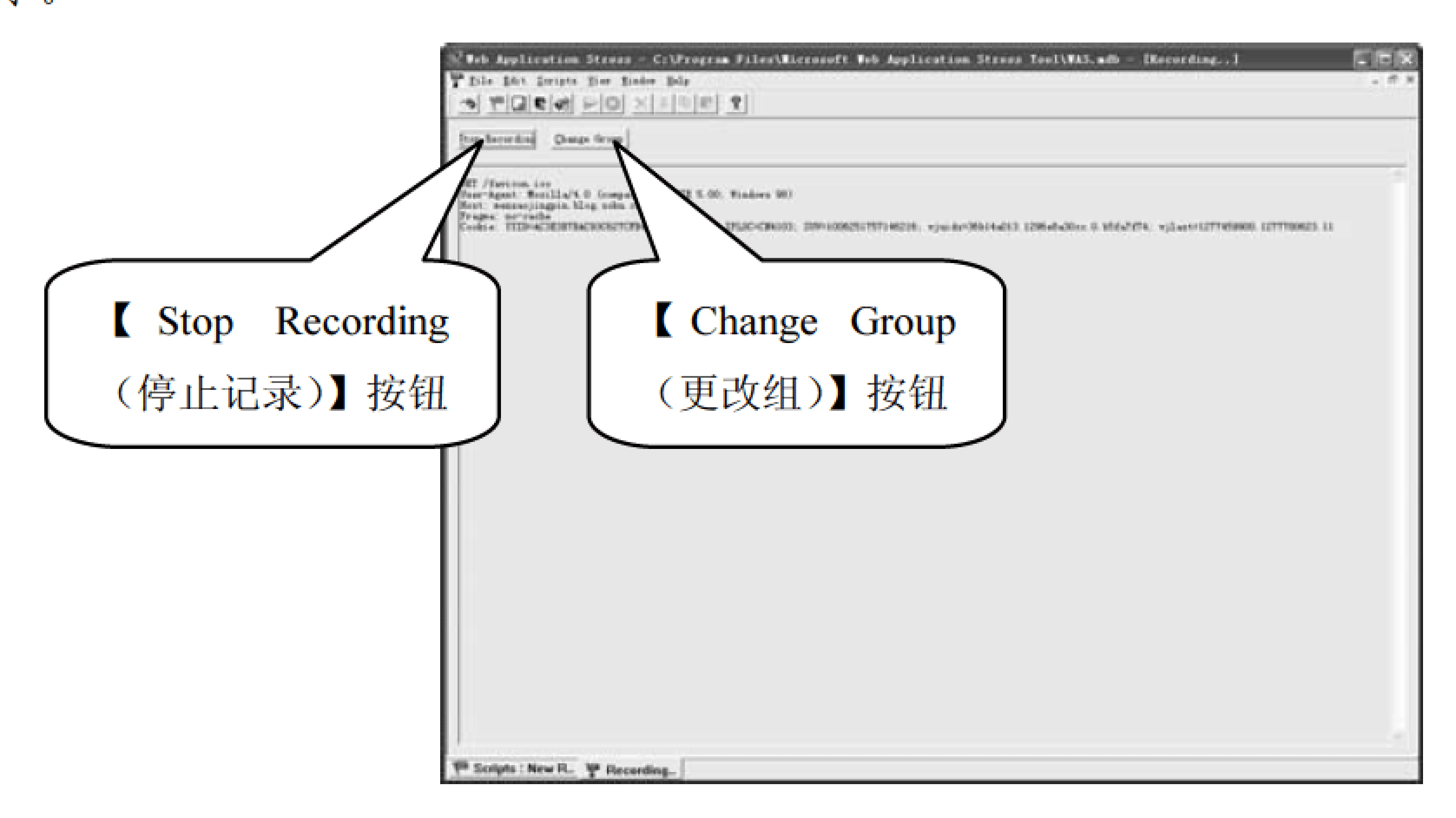


图 17-60

08 单击【Change Group（更改组）】按钮，打开【New Group（新组）】对话框，如图 17-61 所示。在【Group Name（组名）】文本框中输入新建组的名称后，单击【确定】按钮，将计算机组的名称更改为刚设置的名称。

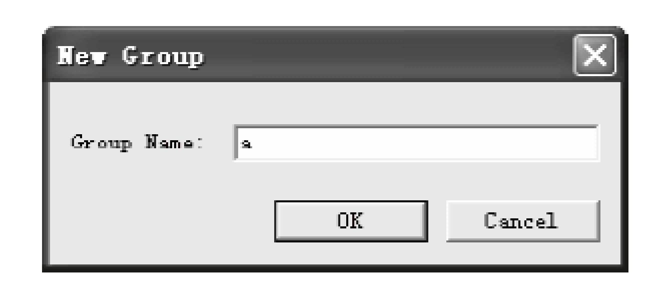


图 17-61

09 当完成了站点浏览后，返回到【WAS】主窗口（如图 17-60 所示），单击【Stop Recording（停止记录）】按钮，即可终止记录并产生一个新的测试脚本，如图 17-62 所示。

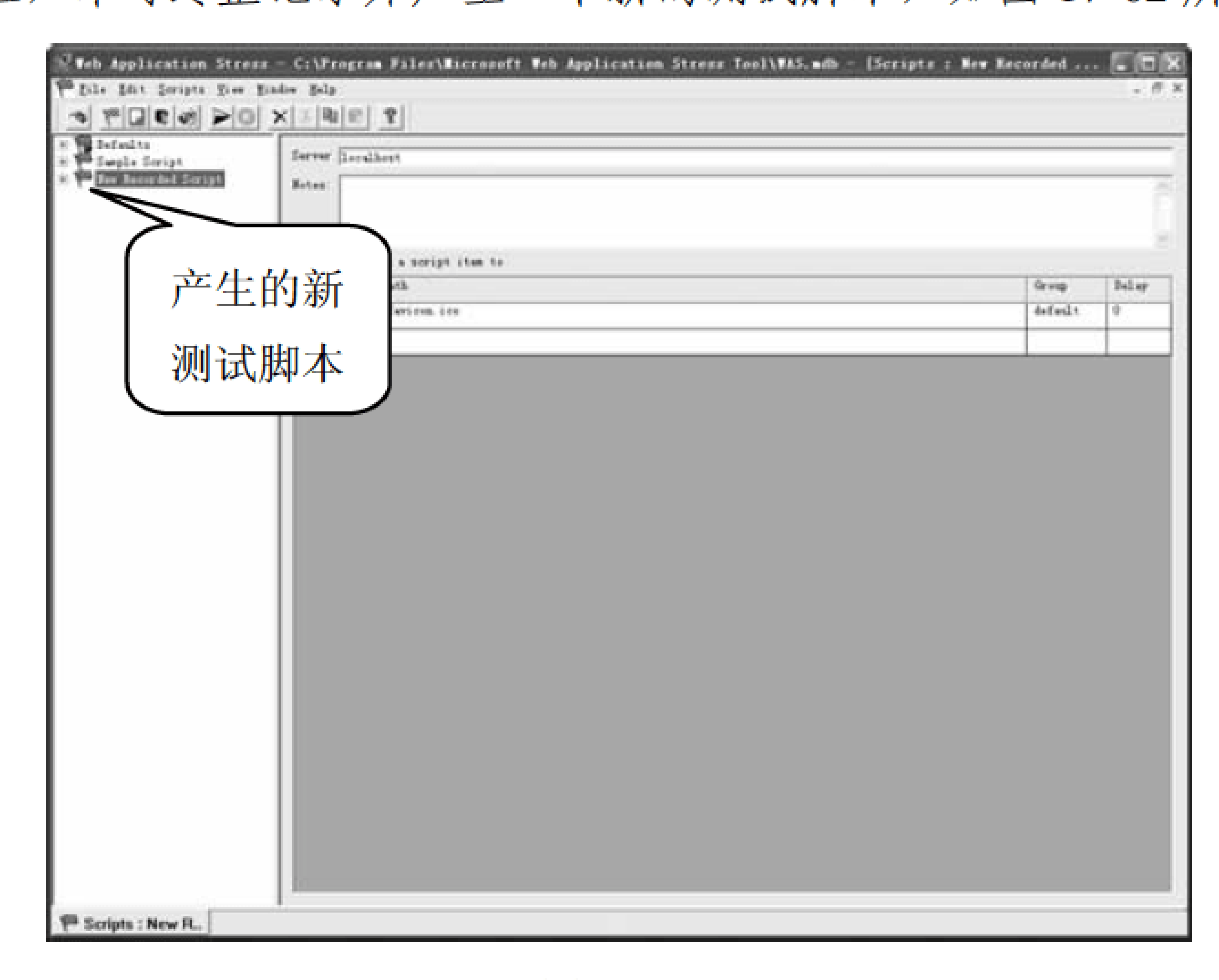


图 17-62

10 为了能更好地运行性能测试，还需要修改测试脚本的设置。如图 17-63 所示，单击左边的【Settings】（设置）选项，在右边窗口中打开【Settings】（设置）窗口。

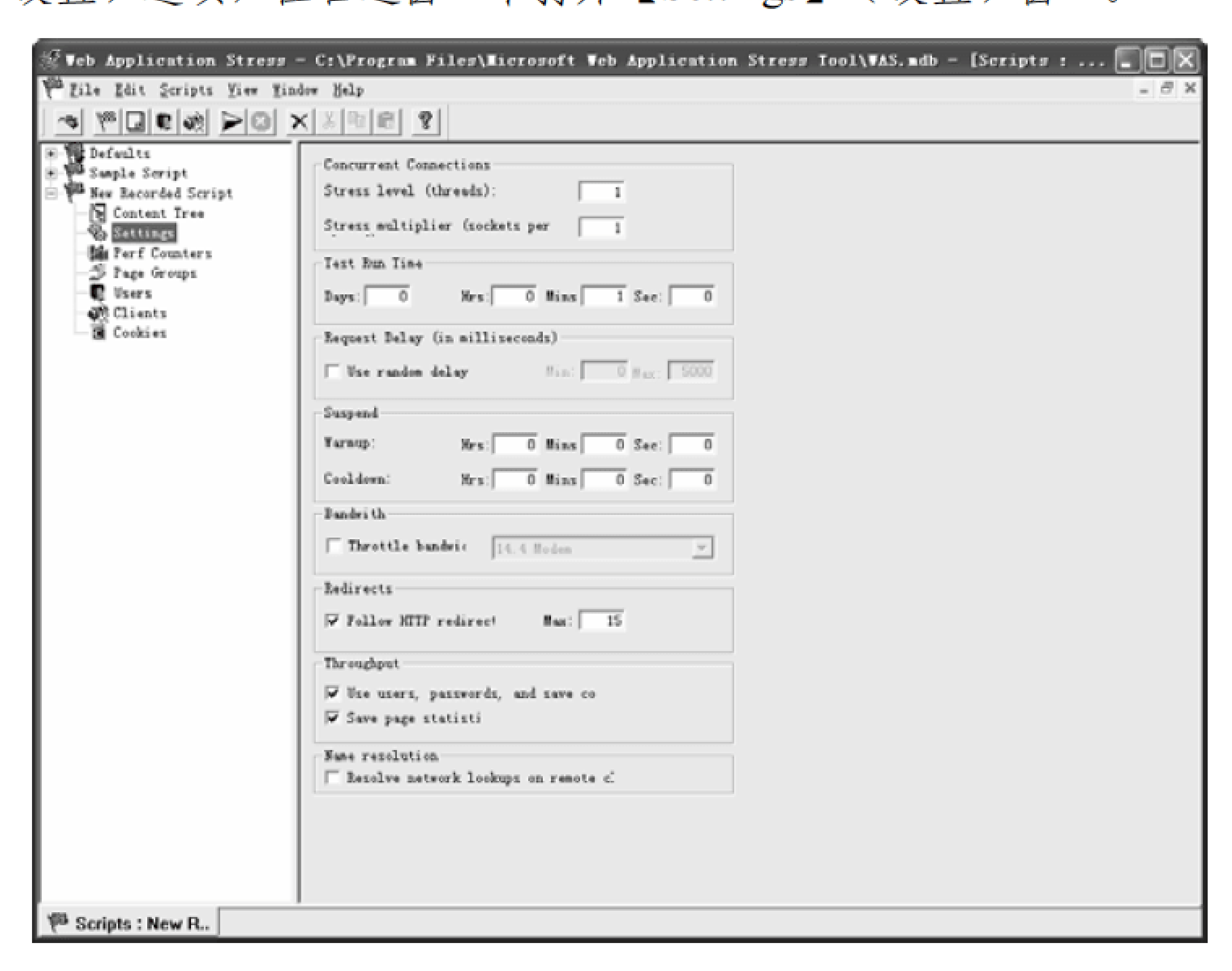


图 17-63

在其中可以设置各种脚本测试指定参数，其各个参数的具体作用如下。

（1）并发连接数

【Concurrent Connections】（并发连接）部分可以指定【Stress level】 (threads)的值和【Stress multiplier】 (sockets per thread)来控制对目标服务器的压力及负载程度。其中【Stress level】是全部客户端所产生的 Windows NT 线程的总数。

（2）测试运行时间

【Test Run Time】（测试运行时间）是以日、小时、分钟、秒来设定总的运行时间。这主要取决于脚本项的预期反应时间，测试程序的反应时间越高，测试进行的时间就应该越长，以便产生大量的数据。建议运行测试脚本至少若干分钟以便产生足够的请求，避免变形的测试结果。

（3）挂起时间

【Suspend】部分是以小时、分钟、秒来设置【Warmup】和【Cooldown】时间。其中【Warmup】时间是初始化测试运行时间，在这段时间里不会收集和计算性能数据；而【Cooldown】时间是指定结束阶段的测试时间，也不收集数据。【Warmup】和【Cooldown】被用于最小化测试结果的失真。

（4）带宽瓶颈

【Bandwidth】(带宽)是模拟从 14.4 Kbps 的 modem 连接到 T1(15.5Mbps)的 Local Area Network (LAN)连接的网络带宽。这个特性的最大优点在于可以支撑大量的并发连接到目标服务器。

11 在【设置】窗口中勾选【Throttle bandwidth】复选框，在弹出的快捷菜单选择一个代表大多数用户的连接吞吐量的带宽即可，如图 17-64 所示。

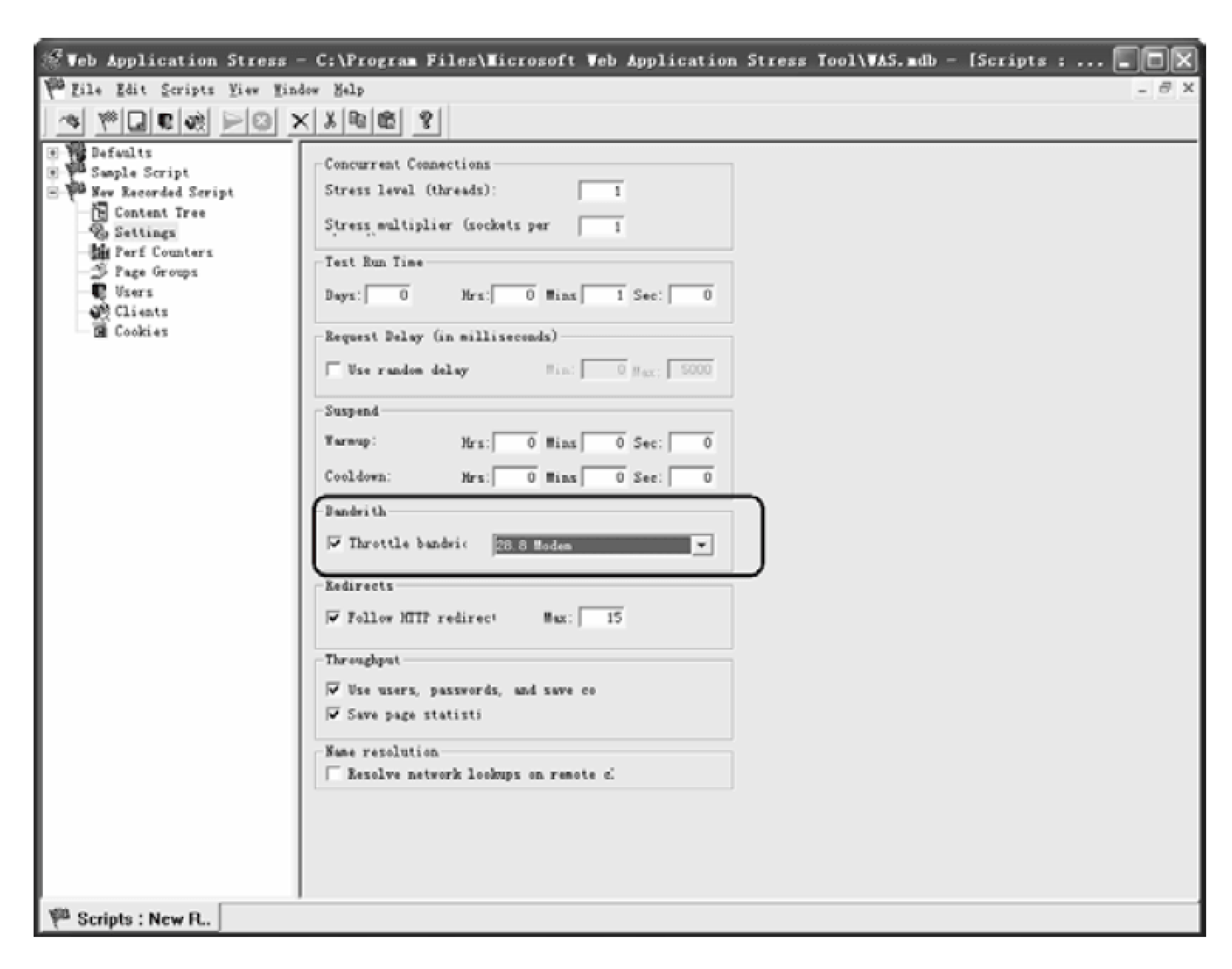


图 17-64

12 若想测试需要署名登录的 WEB 站点时，WAS 提供一个 USERS 特性，可用于存储多个用户的用户名、密码和 cookie 信息。在【WAS】主窗口中选择【View】→【Users】菜单命令，看到默认创建的用户，如图 17-65 所示。

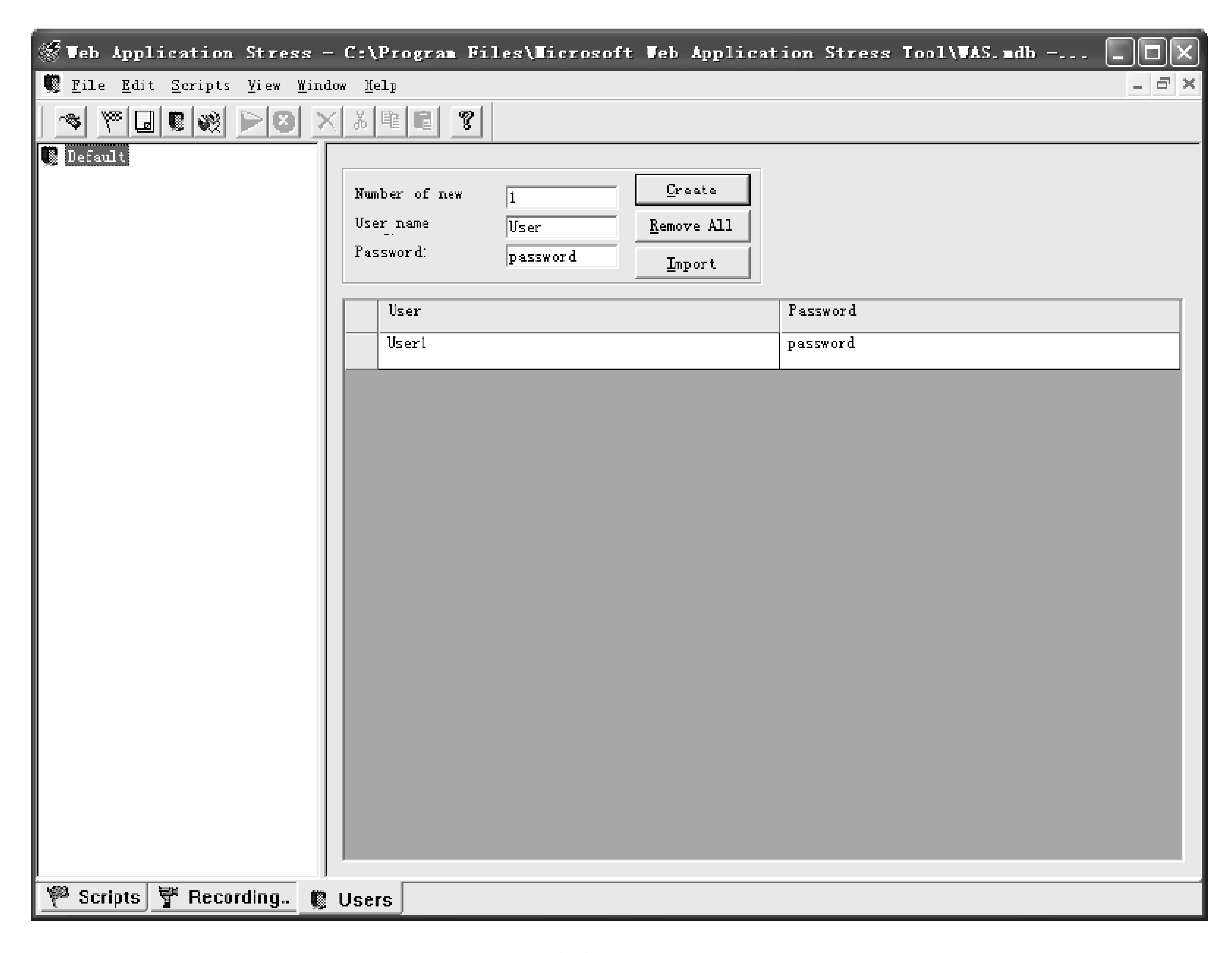


图 17-65

13 如图 17-66 所示，单击【Remove All】按钮，则可清除所有的记录。在【Number of new users】文本框中输入想创建的新用户数量。在【Password】文本框中输入密码，相同的密码会赋值给所有用户，然后单击【Create】（创建）文本框中按钮，创建新的用户。

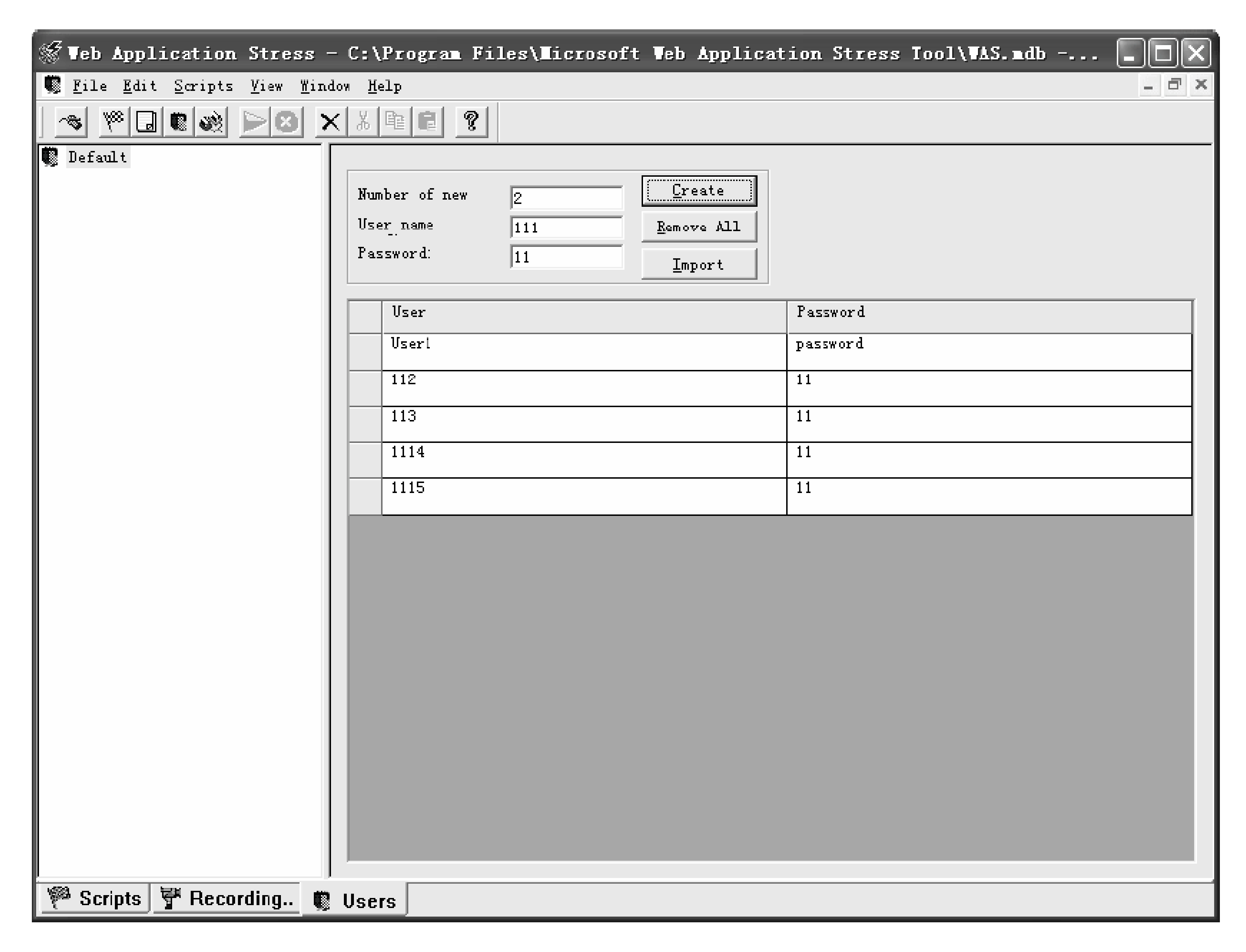


图 17-66

14 设置完成后，选择【Scripts】（脚本）➢【Run】（运行）菜单命令，开始测试，如图 17-67 所示。

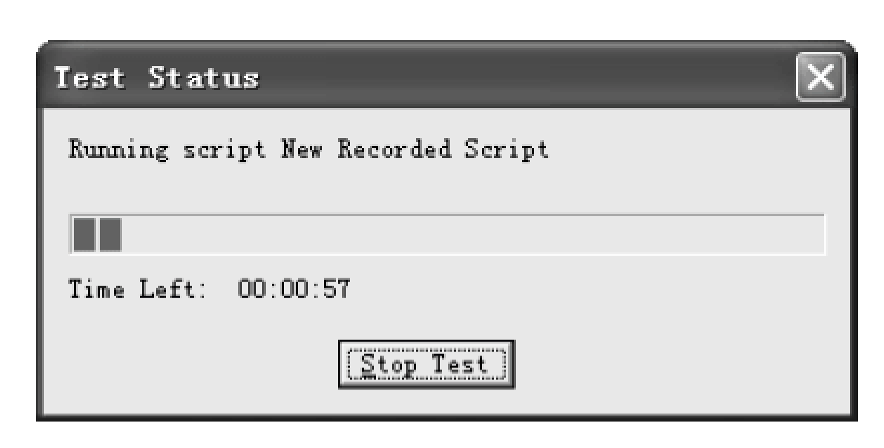


图 17-67

2. 进行数据分析

在测试网站的承受压力后，就可以生成报告，并根据生成的报告进行分析，其具体操作步骤如下。

01 在【WAS】主窗口中选择【View】➢【Reports】菜单命令，打开【报告】窗口，如图 17-68 所示。

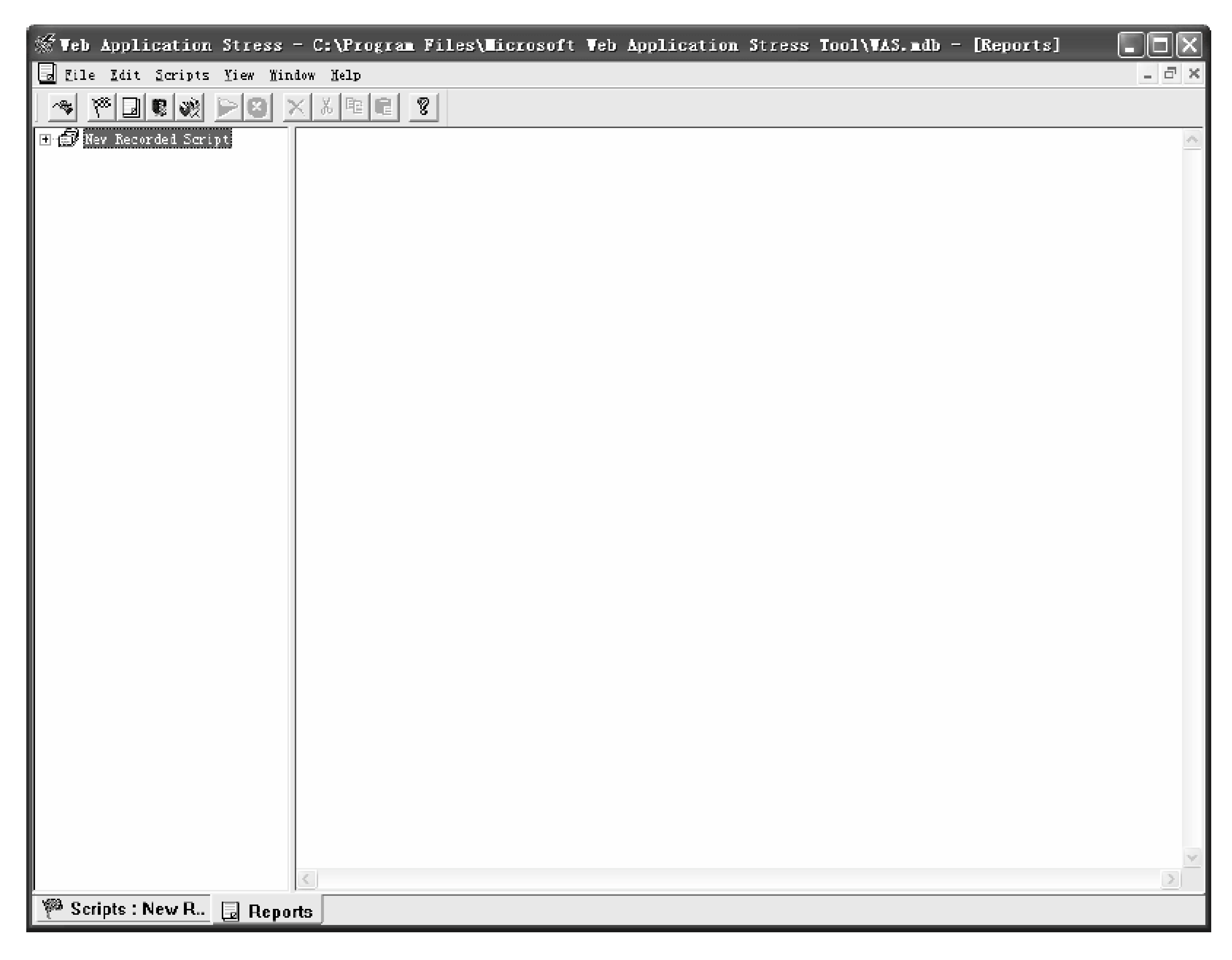


图 17-68

02 在左侧列表中将展开相应的报告，并单击其中的时间，可以看到生成的整个报告的内容，如图 17-69 所示。

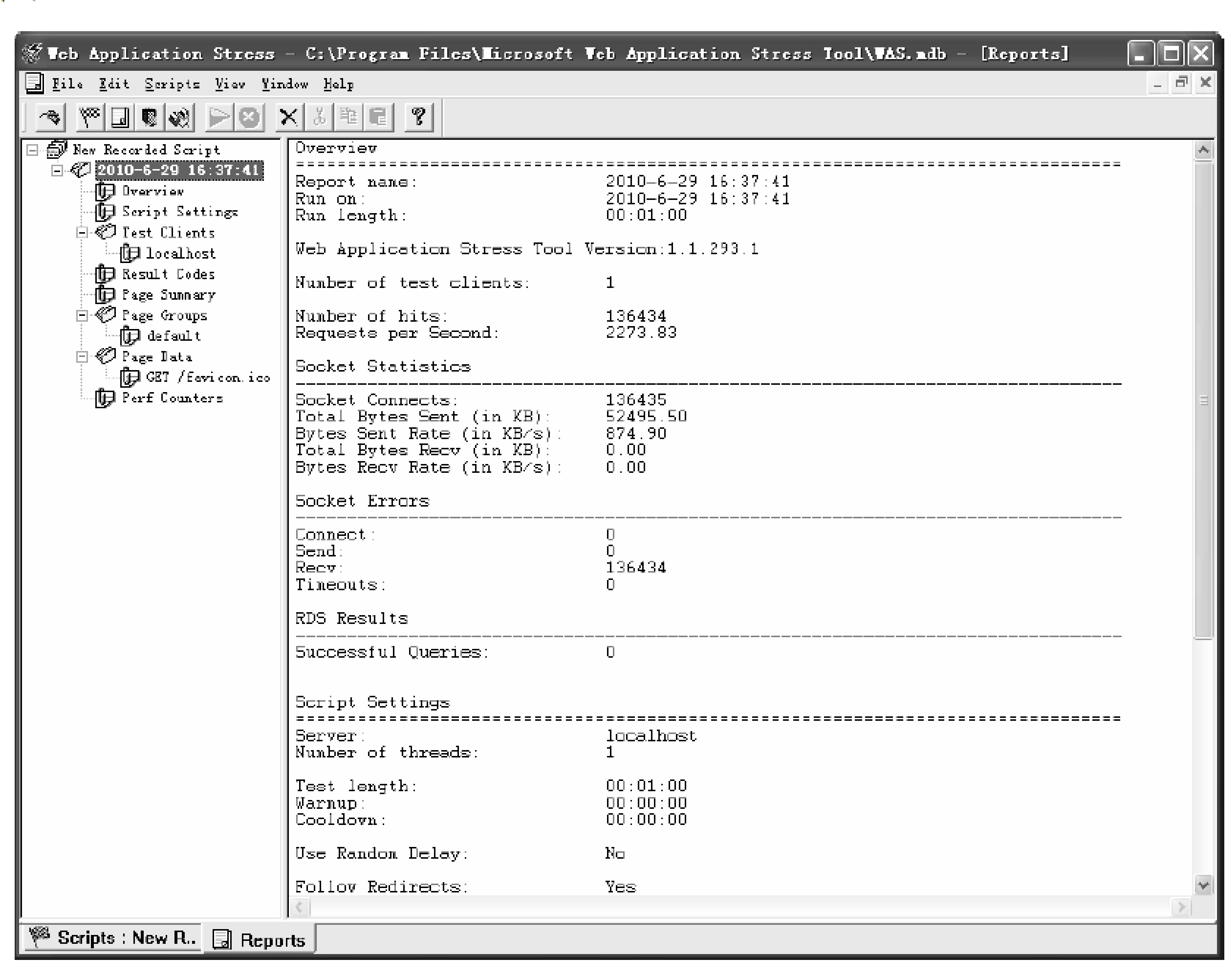


图 17-69

03 单击时间下面的任意选项，查看相应脚本报告的内容，例如单击【OverView】选项，即可看到该脚本对应的报告，如图 17-70 所示。

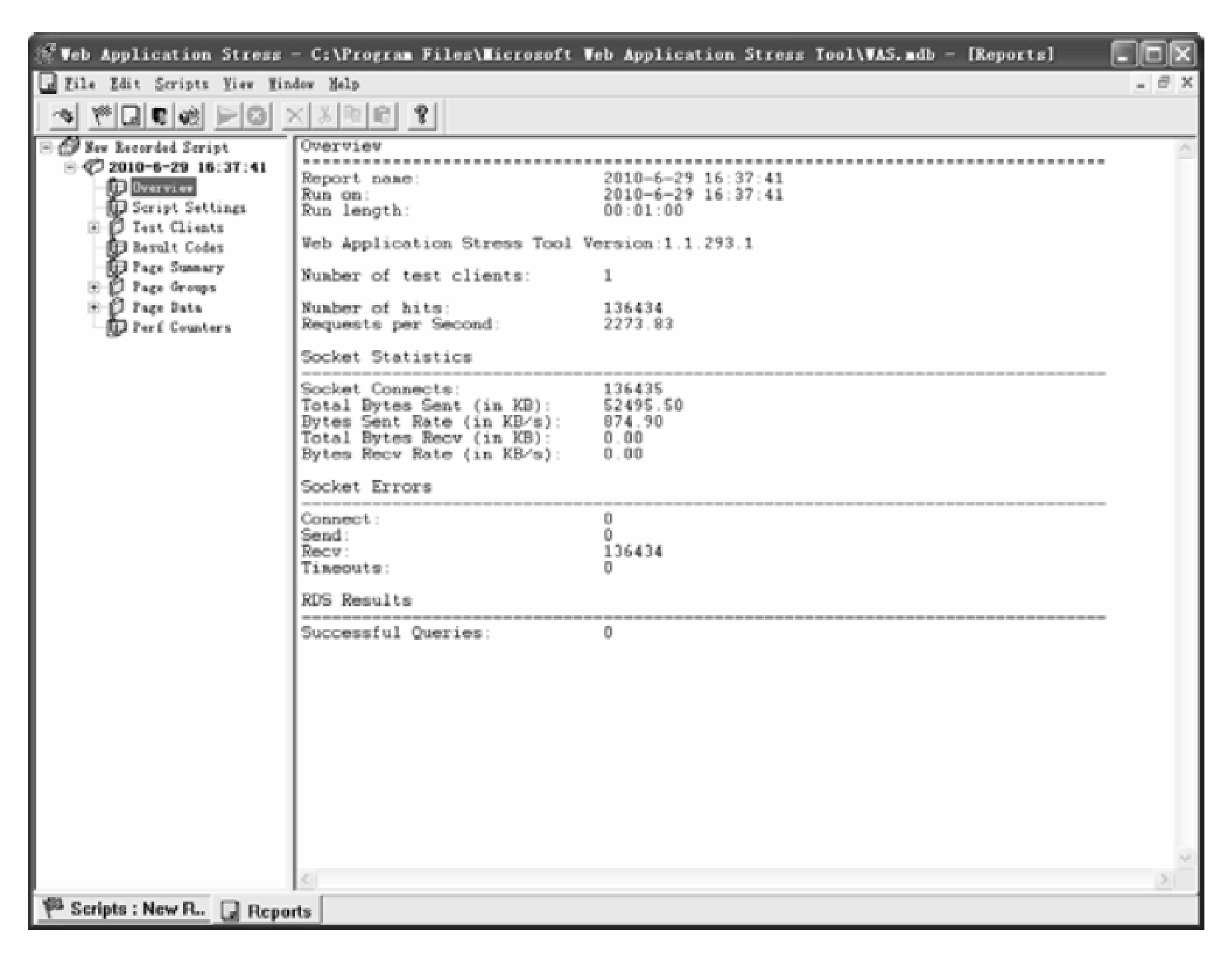


图 17-70

04 可以通过检查 Socket Errors 部分（如图 17-70 所示）是否有任何与 Socket 有关的错误（值不为 0）来判断网站是否正常运行。单击报告列表中的【Page Data】节点，展开所有项目，查看每个脚本项在右边窗口页面数据的报告，找出出现错误的项目，如图 17-71 所示。

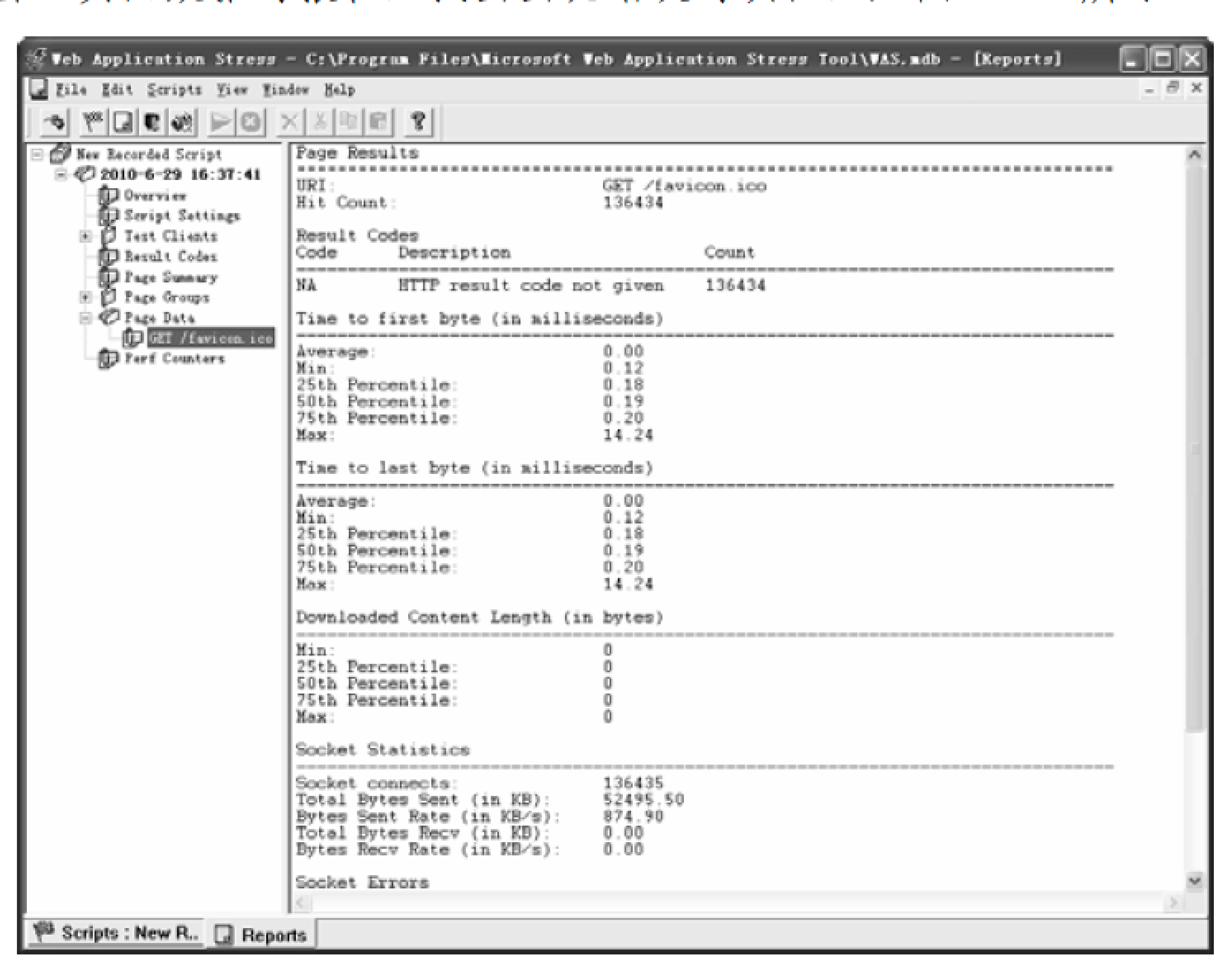


图 17-71

Socket 常见的错误如下：

（1）Connect：客户端不能与服务器取得连接的次数。如果这个值偏高，检查在客户端与服务器之间产生的任何潜在的错误。

（2）Send：客户端不能正确发送数据到服务器的次数。如果这个值偏高，检查服务器是否正

常工作。在客户端打开 IE 浏览器，然后手动点击站点页面，验证站点是否正常地工作。

（3）Recv：客户端不能正确从服务器接收数据的次数。如果这个值偏高，执行和 Send 错误相同的操作，还要检查一下如果降低负载系数，错误是否跟着减少。

（4）Timeouts：超时的线程的数目，且随后就关闭了。如果这个值偏高，在客户端打开 IE 浏览器，然后手工点击站点页面验证是否即使只有一个用户该程序也会很慢，然后做一个不同负载系数的压力测试，来查看程序的潜在特征。

通过不断增减用户数量和改变其他参数测试，可以最大限度地了解网站程序和服务器的承受能力，以便在开始提供服务之前限止访问量及其他参数，保证网站可以正常运行。

17.4.2　检测上传文件的安全性

服务器提供了多种服务项目，其中上传文件是其提供的最基本的服务项目。它可以让空间的使用者自由上传文件，但是在上传文件的过程中，很多用户可能会上传一些对服务器造成致命打击的文件，如最常见的 ASP 木马文件。所以网络管理员必须利用入侵检测技术来检测网页木马是否存在，以防止随时随地都有可能发生的安全隐患，思易 ASP 木马追捕就是一个很好的检测工具，通过该工具可以检测到网站中是否存在 ASP 木马文件。

下面介绍使用思易 ASP 木马追捕来检测上传文件是否为木马的过程，其具体的操作步骤如下。

01 下载思易 ASP 木马追捕 2.0 源文件，并将 asplist2.0.asp 文件存放在 IIS 默认目录【C:\Inetpub\wwwroot】，然后在【管理工具】窗口中双击【Internet 信息服务】按钮，打开【Internet 信息服务】窗口，如图 17-72 所示，双击【默认网站】图标，在右边列表中即可看到添加的 asplist2.0.asp 文件并选中。

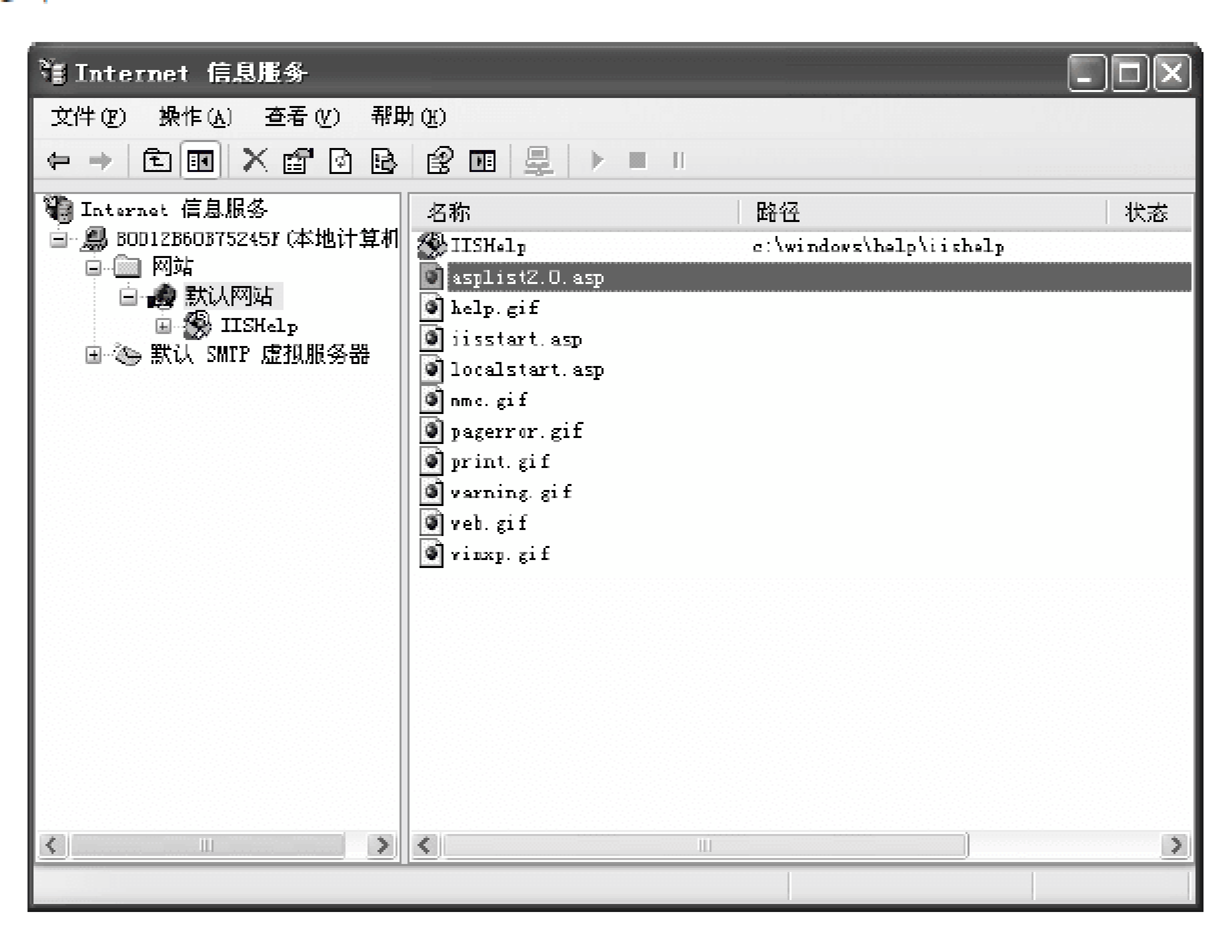


图 17-72

02 单击鼠标右键，在弹出的快捷菜单中选择【浏览】选项，在 IE 浏览器中打开该网页，在【检查文件类型】后面的文本框中输入思易 ASP 木马追捕可以检查的文件类型，主要包括：ASP、JPG、ZIP 在内的许多种文件类型，默认是检查所有类型。在【增加搜索自定义关键字】文本框中输入确定 ASP 木马文件所包含的特征字符，以增加木马检查的可靠性，关键字用“、”隔开，如

图 17-73 所示。

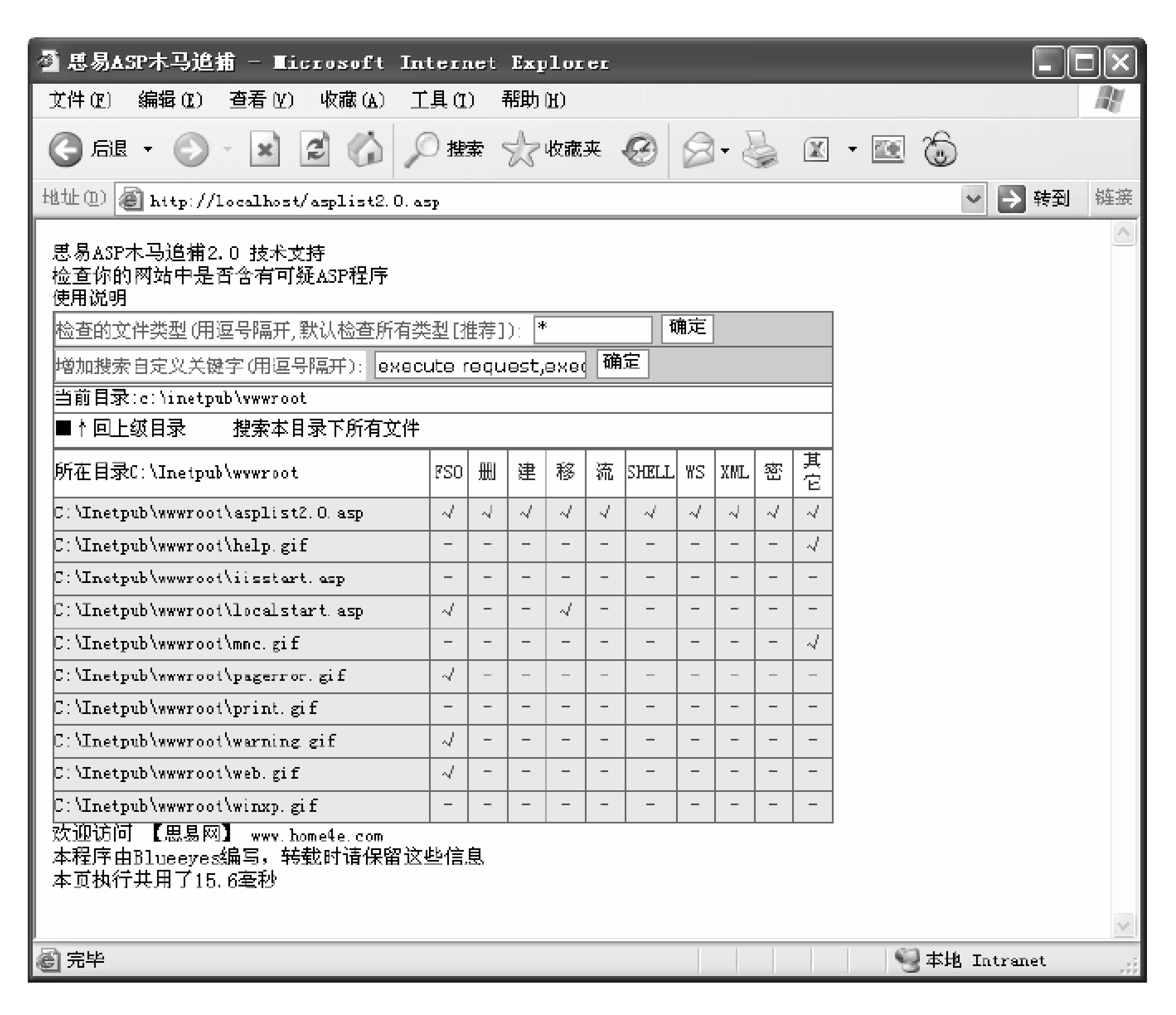


图 17-73

03 在【所在目录】中列出了当前浏览器的目录，上面显示的是该目录包含的子目录，下面显示是该目录的文件。此时单击目录列表中的目录可以检查相应的目录，而单击【回到上级目录】链接按钮即可返回到当前目录的上一级目录，如图 17-74 所示。

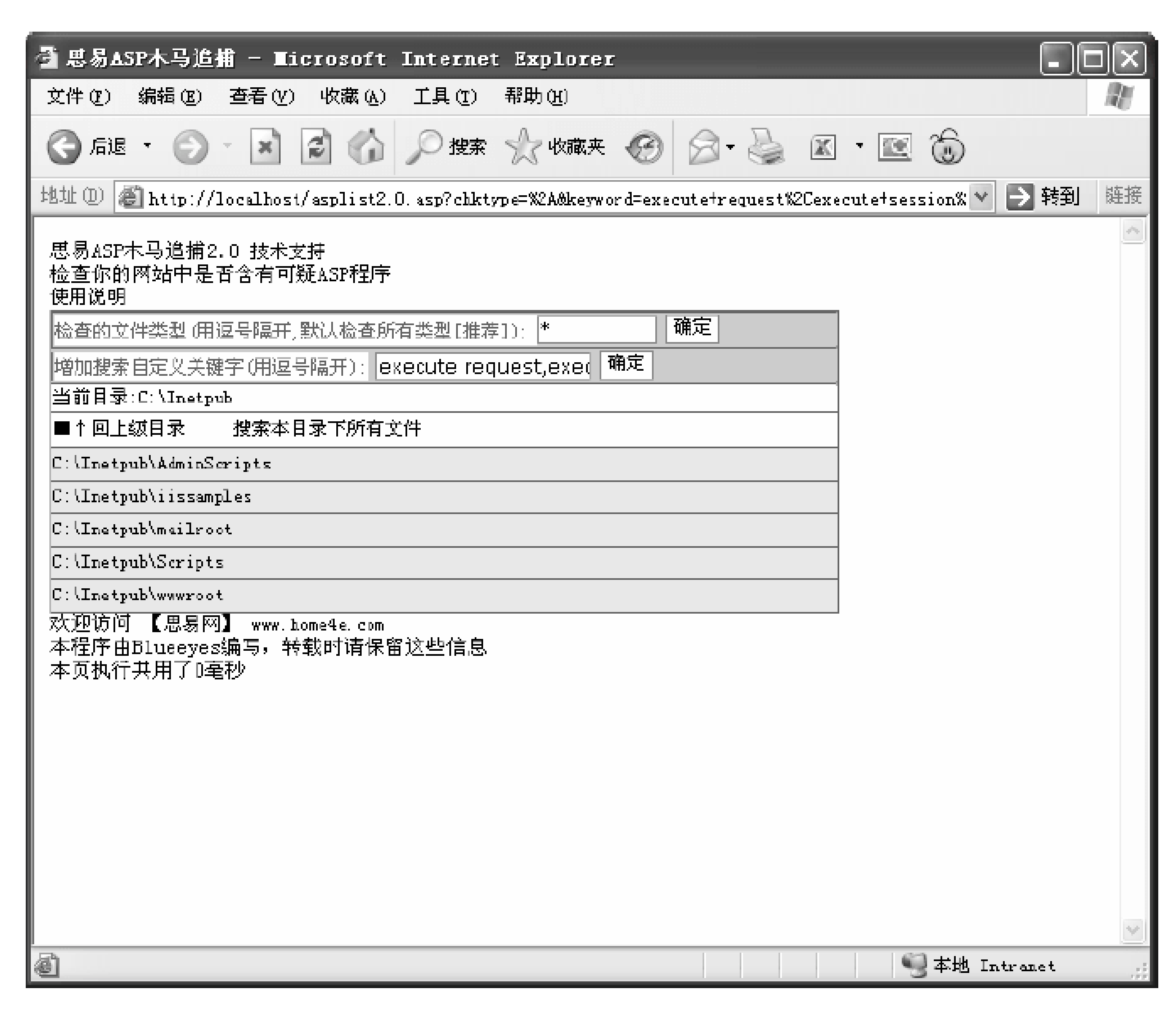


图 17-74

04 如图 17-75 所示，在设置好【检查文件类型】和【增加搜索自定义关键字】属性后，单击【确定】按钮，根据设置进行网页木马的探测。

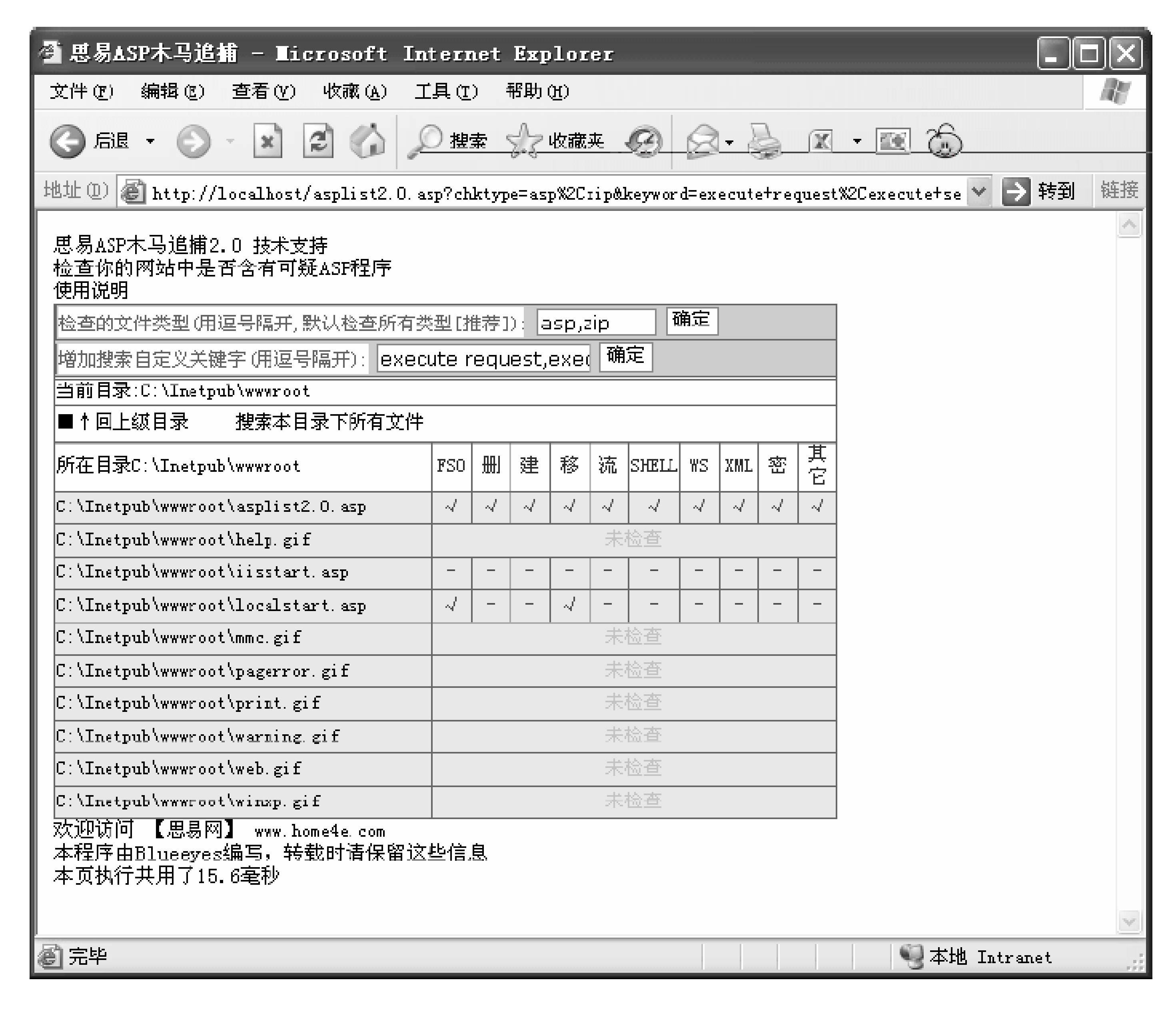


图 17-75

05 在【思易 ASP 木马追捕】工具中可以查看目录下的每一份文件，正常的网页文件一般不会支持删除、新建、移动文件的操作。如果检测出来的文件支持删除、新建操作或同时支持多种组件的调用，则可以确定该文件为木马病毒，直接删除即可。

图 17-75 中各个参数的含义如下。

- FSO：FSO 组件，具有远程删除、新建、修改文件或文件夹的功能；
- 删：可以在线删除文件或文件夹；
- 建：可以在线新建文件或文件夹；
- 移：可以在线移动文件或文件夹；
- 流：是否调用 Adodb.stream；
- Shell：是否调用 Shell，Shell 是微软对一些常用外壳操作函数的封装；
- WS：是否调用 WSCIPT 组件；
- XML：是否调用 XMLHTTP 组件；
- 密：网页源文件是否加密。

17.5　专家答疑

（1）在计算机中安装了入侵检测系统，为什么只能监听到本机的信息？该系统会不会影响网络速度呢？

答：如果只能检测到本机的信息，则说明本机所处的网络是用交换机连接的。如果想要监控局域网中的其他电脑的通信信息，那么需要增加一个 HUB（集线器）或者支持端口镜像的交换机。

若是通过服务器上网的话，也可以直接把 HUB 或支持端口镜像的交换机安装在服务器上。在计算机上安装入侵检测系统，不会影响局域网的网速。因为，现在大多数入侵检测系统都采用旁路监控的模式，只对数据包的拷贝进行分析。

（2）在计算机中安装了 Sax 入侵检测系统，为什么什么都监控不到?

答：出现这样的情况，可能与监听的网卡有关。打开 Sax 入侵检测系统的【配置】界面，选择【监听设备】下拉框，如果有两个或两个以上的网卡，则检查现在选中的网卡是不是正在使用的网卡。如果监听设备中没有找到任何网卡或者信息不正确，则说明用户安装的 Sax 入侵检测系统有问题，应卸载后重新安装。如果仍然看不到网卡，那么有可能该网卡不支持该入侵检测系统。

（3）入侵检测系统如何与网络中的其他安全措施相配合？

答：在使用入侵检测系统的同时还需要采取一些措施，例如建立不断完善的安全策略；根据不同的安全要求，合理放置防火墙；使用网络漏洞扫描工具检查防火墙的漏洞；使用主机策略扫描工具以确保服务器等关键设备的最大安全性；使用入侵检测系统和其他数据包嗅探软件查看网络上是否存在入侵活动；使用基于主机的入侵检测系统和病毒扫描软件对成功的入侵行为作标记；使用网络管理平台为可疑活动设置报警等。